IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

BEFORE THE HONORABLE SPENCER WILLIAMS, JUDGE

ROGER SCHLAFLY, PLAINTIFF, VS. PUBLIC KEY PARTNERS AND RSA DATE SECURITY, INC., DEFENDANTS.	NO. C-94-20512 SW
RSA DATA SECURITY, INC., PLAINTIFF, VS. CYLINK CORPORATION AND CARO-KANN CORPORATION, ET AL., DEFENDANTS.	NO. C-96-20094 SW
	SAN JOSE, CA TUESDAY OCTOBER 1, 1996 VOLUME 1 PAGES 1 - 153 MARKMAN HEARING

ORIGINAL

238

FILED

MAR 05 1997

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

APPEARANCES:

FOR THE PLAINTIFF ROGER SCHLAFLY:
DR. ROGER SCHLAFLY:
P.O. BOX 1680
SOQUEL, CA 95073

APPEARANCES CONTINUED ON NEXT PAGE

COURT REPORTER: JEANNETTE L. BUSH, CSR #10572
COURT REPORTER

COMPUTERIZED TRANSCRIPTION BY PREMIER POWER

APPEARANCES: (CONTINUED)

FOR RSA DATA SECURITY, INC.:
HELLER, EHRMAN, WHITE & MC AULIFFE
525 UNIVERSITY AVENUE
PALO ALTO, CA 94301-1900
BY: ROBERT T. HASLAM
ROBERT D. FRAM
BETH MITCHELL
ATTORNEYS AT LAW

FOR CYLINK CORPORATION, CARO-KANN CORPORATION AND STANFORD UNIVERSITY:
MORRISON & FOERSTER, LLP
755 PAGE MILL ROAD
PALO ALGO, CA 94304-1018
BY: KARL J. KRAMER
JANA G. GOLD
ATTORNEYS AT LAW

MORRISON & FOERSTER, LLP
345 CALIFORNIA STREET
SAN FRANCISCO, CA 94104
BY: RAOUL D. KENNEDY
ATTORNEY AT LAW

ALSTON & BIRD
ONE ATLANTIC CENTER
1201 W. PEACHTREE STREET
ATLANTA, GEORGIA 30306
BY: PATRICK J. FLINN
ATTORNEY AT LAW

I N D E X

E X H I B I T S

TUESDAY, OCTOBER 1, 1996 9:40 A.M.

THE COURT: I APOLOGIZE THAT OUR FAST START WAS NOT SO FAST THIS MORNING. I'M SURE WE CAN MAKE IT. NOW, WHERE DO WE GO TODAY? ANY SUGGESTIONS?

MR. FRAM: YES, YOUR HONOR. ROBERT FRAM FOR RSA. WE CONCUR, AND WE HAVE A SUGGESTION THAT WE HOPE WILL DISPOSE OF THE EVIDENTIARY PART OF THE MARKMAN HEARING TODAY EVEN GIVEN THE 3:00 O'CLOCK TERMINATION TIME.

THE COURT: WE'LL BE HERE TOMORROW, TOO.

MR. FRAM: GIVEN THE WITNESSES SCHEDULES AND EVERYTHING ELSE, BY PUTTING THE WITNESSES FIRST, IN FACT, WE WOULD BE ABLE TO GET THE WITNESSES ON AND OFF IN ONE DAY. OUR THINKING IS AS TO THE DOCUMENTS THE PARTIES WANT TO MOVE INTO EVIDENCE, THAT THE PARTIES WOULD MOVE AT THE END OF THE DAY. WE'D MARK THEM OF COURSE AS WE GO --

THE COURT: EXCUSE ME.

(PAUSE IN PROCEEDING.)

MR. FRAM: OUR PROPOSAL IS REAL SIMPLE. WHAT WE SUGGEST IS THAT THE WITNESSES WHO ARE HERE TODAY -- WE PUT THEM UP. WE HAVE THE WITNESSES TODAY. WE MOVE THE DOCUMENTS IN AT THE END OF THE DAY. WE MARK THEM OF COURSE AS WE GO ALONG, THAT THEY GET MOVED IN AT

THE END.

TO EXPEDITE MATTERS, THAT THE OBJECTIONS TO THE DOCUMENTS BE ON PAPER. WE'VE ALREADY SUBMITTED ON A BRIEF, I BELIEVE, A FAIR NUMBER OF THE EVIDENTIARY OBJECTIONS, THIS BEING AN EVIDENTIARY PROCEEDING, THE PARTIES ARE WILLING TO GO THAT WAY.

THERE MAY BE SOME ADDITIONAL EVIDENTIARY OBJECTIONS THAT ARE NOT IN THE BRIEF TO DOCUMENTS THAT WERE NOT PRESENT WHERE THERE WAS NO REQUEST FOR NOTICE. THE PARTIES WILL PROBABLY WANT A FEW DAYS TO PUT IN ANY SUPPLEMENTAL PAPERS ON OBJECTIONS FOR ANYTHING THAT EITHER PARTY HAS TO MOVE AGAINST.

SO THE MOVING WILL EITHER BE SUBJECT TO THE PAPERS ALREADY SUBMITTED OR PAPERS TO BE SUBMITTED WITHIN A FEW DAYS. AND THAT REALLY IN AN EXPEDITIOUS WAY, WE THINK, WILL TAKE CARE OF THE EVIDENTIARY PART OF THE HEARING BECAUSE WE'LL NOT HAVE TO BE DISTRACTED WITH EVIDENTIARY OBJECTIONS ON DOCUMENTS DURING THE COURSE OF THE DAY, AND WE CAN FOCUS ON THE WITNESSES WHO ARE HERE.

MR. FLINN: THE ONLY OTHER THING I WOULD ADD, YOUR HONOR, IS WE WEREN'T QUITE SURE HOW THE COURT WANTED TO HANDLE THE MARKING OF EXHIBITS. SO WHAT WE HAVE DONE IS DIVIDE UP THE NUMBERS, AND WE WILL PROCEED BASED UPON THE DEPOSITION EXHIBITS THAT HAVE

BEEN MARKED SO FAR, AND THEN THE PARTIES WILL DIVIDE UP THE NUMBERS.

RSA WILL TAKE THE NUMBERS FROM 500 TO 1000. CYLINK AND CARO-KANN WILL TAKE THE NUMBERS BETWEEN 0 AND 499, AND MR. SCHLAFLY WILL TAKE THE NUMBERS ABOVE 1500 I BELIEVE; IS THAT CORRECT?

THE DEPOSITION EXHIBITS HAVE ALREADY BEEN MARKED UP THROUGH ABOUT 66, AND WE'LL USE THOSE NUMBERS FROM THE DEPOSITIONS THEMSELVES. AND THEN I BELIEVE RSA WILL TAKE 1000 ABOVE, AND WE WILL TAKE 500 AND ABOVE FOR NEW EXHIBITS, AND MR. SCHLAFLY WILL TAKE 1500 AND ABOVE.

THE COURT: ANYTHING AGREED ON IS AGREEABLE TO ME.

MR. FRAM: APPRECIATED, YOUR HONOR. WHAT THAT WILL LEAVE IS A QUESTION OF POST HEARING BRIEFING ON THE EVIDENCE OF RECORD AND THE QUESTION OF ARGUMENT OF WHEN THE COURT WOULD LIKE TO HAVE THAT. WE'RE AVAILABLE TOMORROW.

WE HAVE THE MOTION TO REMAND ON CALANDER FOR TOMORROW. WE COULD PROCEED WITH THAT. IF THE COURT WANTS ARGUMENT TOMORROW, WE COULD PROCEED AT THAT TIME ON THE MARKMAN ISSUES AS WELL. IF THE COURT WOULD LIKE TO PUT STALL ON THAT UNTIL AFTER RECEIVING A POST HEARING BRIEF ON THE EVIDENCE OF RECORD, WE'D BE HAPPY

TO DO THAT OF COURSE WITH PLEASURE.

THE COURT: WELL, IF WE COULD WRAP UP THIS PORTION TOMORROW, THEN BE CLEAR FOR THE REST OF THE TIME TO DEVELOP THE REST OF THE MATTER FOR PREPARATION OF TRIAL AND SO FORTH. IF WE CAN, WE'LL DISPENSE WITH THE WITNESSES WHO ARE HERE AND ANYTHING ELSE THAT MIGHT WANT TO BE SUBMITTED.

APPARENTLY, THERE ARE SOME WITNESSES YOU WANT TO PRESENT. WITNESSES THAT ARE SUPPOSED TO BE HERE. ARE THERE SOME WITNESSES THAT SOMEONE WANTS TO PRESENT THAT ARE NOT NAMED AND PREPARED?

MR. FRAM: THERE MAY BE AN ISSUE -- AS TO THE COURT'S QUESTION, THERE MAY BE A QUESTION AS TO ONE WITNESS WHO MIGHT BE CALLED. MY SUGGESTION IS WE TAKE THAT MATTER UP IF THAT WITNESS IS CALLED AT THAT TIME.

THE COURT: OKAY.

MR. FRAM: BUT THE QUESTION -- I GUESS THE COUNSEL IS CURIOUS AS TO WHAT TOMORROW IF THE COURT WOULD LIKE TO HAVE ARGUMENT BY COUNSEL ON THE CLAIM CONSTRUCTION QUESTIONS AS TO WHICH EVIDENCE IS PRESENTED TODAY OR WHETHER THE COURT WOULD LIKE TO WAIT UNTIL AFTER A POST HEARING PAPER IS PROVIDED. IT'S A QUESTION OF JUST TIMING ON THE ARGUMENT.

MR. KENNEDY: LET ME ADDRESS THAT, YOUR HONOR. IT'S CYLINK AND CARO-KANN AND STANFORD'S

POSITION THAT WE'RE HERE TODAY AND TOMORROW TO ADDRESS THOSE ISSUES, AND WE DON'T WANT TO PUT THEM OFF FOR FURTHER BRIEFING. WE HAVE BRIEFED THEM. WE ARE PREPARED TO DISCUSS THEM WITH THE COURT.

THE COURT: IF I WANT TO GET ANY FURTHER ARGUMENT, I'LL ASK TO SUBMIT IT IN WRITING.

MR. FRAM: WE'RE COMPLETELY HAPPY TO GO THAT WAY, YOUR HONOR. I GUESS THE ONE SMALL POINT -- I THINK WE'RE GOING TO HAVE TO DECIDE THIS NOW -- IS I THINK THE PARTIES MAY BE OF DISAGREEMENT IS THAT RSA HAS REQUESTED AN OPPORTUNITY ALSO TO PUT ANY POST HEARING BRIEF TO BE ABLE TO ARGUE THE EVIDENCE OF RECORD, AND THAT'S, I THINK, THE LAST DETAIL, AND WE'RE READY TO GO WITH THE ORAL ARGUMENT TOMORROW.

THE COURT: IF I WANT FURTHER ARGUMENT, I'LL HAVE THE ARGUMENT TOMORROW. IF I WANT FURTHER BRIEFING, I'LL ASK FOR IT. IF I DON'T NEED IT, I DON'T NEED IT.

MR. FRAM: FINE, YOUR HONOR.

MR. KENNEDY: THANK YOU, YOUR HONOR.

THE COURT: NOW, ANYTHING ELSE ON OPENING UP RIGHT NOW?

MR. KENNEDY: YES, YOUR HONOR. RAOUL KENNEDY ON BEHALF OF CYLINK. I UNDERSTAND THAT PROFESSOR CONHEIM HAS TEACHING OBLIGATIONS TOMORROW, AND THERE'S

BEEN A REQUEST THAT HE BE CALLED AS THE FIRST WITNESS IN THE CASE, AND WE HAVE NO OBJECTION WHATSOEVER TO THAT, THAT MAKES TOTAL SENSE.

OUR ONLY REQUEST WOULD BE THAT WE TRY TO GET SOME GROUND RULES BECAUSE I'M STILL NEW TO THIS MARKMAN PROCEEDING, AND I'M STILL HAVING TROUBLE REMEMBERING THAT EXPERT TESTIMONY IS TESTIMONY OF LAST RESORT IN THESE KINDS OF A HEARING, THAT THE FEDERAL CIRCUIT TELLS US THAT THE FIRST LEVEL OF EVIDENCE IS INTRINSIC EVIDENCE, THE PATENT, ET CETERA.

THE COURT: THAT'S RIGHT.

MR. KENNEDY: IF FOR ANY REASON THAT DOESN'T DO THE JOB, THEN WE TURN TO WRITTEN EXTRINSIC EVIDENCE -- DICTIONARIES, TREATISES, THAT SORT OF THING AS YOUR HONOR KNOWS.

AND AS THE VITRONICS OPINION IN 90 F.3RD, PAGE 1576 TOLD US JUST THIS SUMMER, EXPERT TESTIMONY MAY ONLY BE RELIED UPON IF THE PATENT DOCUMENTS TAKEN AS A WHOLE ARE INSUFFICIENT TO ENABLE THE COURT TO CONSTRUE DISPUTED CLAIM TERMS. SUCH INSTANCES WILL RARELY IF EVER OCCUR.

AND OF COURSE THE COURT IN THIS CASE WENT ON TO REVERSE THE DISTRICT JUDGE FOR HAVING ERRONEOUSLY RELIED ON EXPERT TESTIMONY. THE VITRONICS OPINION GOES ON TO CAUTION THAT EVEN IN THOSE RARE INSTANCES,

WHERE EXPERT TESTIMONY IS APPLICABLE, IT SHOULD BE VIEWED IN THEIR WORDS, NOT MINE, WITH CAUTION BECAUSE IT'S NOT PART OF THE PUBLIC RECORD THAT WAS AVAILABLE BEFOREHAND. AND TO AGAIN QUOTE, "IT'S NO BETTER THAN OPINION TESTIMONY ON MEANING OF STATUTORY TERMS."

NOW, AGAINST THAT BACKGROUND, WE'RE SOMEHOW TOLD THAT THIS, IN FACT, IS ONE OF THOSE RARE OCCURANCES, AND IN FACT IT'S SO RARE THAT WE'RE GOING TO SPEND A FULL DAY ON LAST RESORT TESTIMONY. NOW, WHAT THAT SAYS IS THE SPONSORS OF LAST RESORT TESTIMONY HAVE BEEN THROUGH THE PATENT, BEEN THROUGH THE PROSECUTION HISTORY, COMBED THE TECHNICAL LITERATURE, AND CAN'T FIND SUPPORT FOR THEIR POSITION AND HAVE SAID, "WOOPS, WE'RE GOING TO HAVE TO GO TO THE LAST RESORT. LET'S GET SOME EXPERTS."

NOW, MAYBE THIS IS ONE OF THOSE RARE SITUATIONS AND IN FACT SO RARE THAT WE HAVE TO LAST RESORT FOR AN ENTIRE DAY. BUT I SUGGEST THAT AT A MINIMUM, SOME SORT OF OFFER OF PROOF OUGHT TO BE ADVANCED AS TO WHY IT IS THAT THIS FALLS WITHIN THAT RARE SITUATION, AND IN PARTICULAR WHAT IT IS THAT THESE EXPERTS ARE GOING TO DO TO BE OF ASSISTANCE TO THE COURT RATHER THAN TRYING TO BACKDOOR SOME INADMISSIBLE TESTIMONY.

WE TOOK PROFESSOR KONHEIM'S DEPOSITION, AND

HE'S NOT A PATENT LAWYER, AND I DON'T MEAN TO CRITICIZE HIM OR ACCUSE HIM OF DOING ANYTHING INTENTIONALLY WRONG. BUT HE CANDIDLY ADMITTED THAT WHAT HE THOUGHT HE WAS SUPPOSED TO DO AND WHAT HE IN FACT DID WAS TO READ THE CLAIMS AGAINST THE LANGUAGE OF THE SPECIFICATIONS AND HAS IMPORTED LIMITATIONS FROM THE SPECIFICATIONS INTO THE CLAIMS WHICH AS WE ALL KNOW FOR A LAWYER OR A COURT IS A NO, NO.

NOW PRESUMABLY PROFESSOR KONHEIM HAS BEEN WOODSHEDED SINCE HIS DEPOSITION AND WILL BE UP HERE TO PROVIDE SOMETHING ELSE. BUT BEFORE WE SPEND A WHOLE DAY ON BOTH RARE AND MINIMAL VALUE TESTIMONY, CAN'T WE GET SOME KIND OF GROUND RULES OR SOME SHOWING FROM THE PROPONENTS AS TO WHY THIS IS THAT HAILEY'S COMET OF A CASE THAT IT IS SO RARE AND THAT WOULD BE MY REQUEST.

THE COURT: I SHOULD HERE THE INTRINSIC EVIDENCE FIRST AND DECIDE WHETHER OR NOT EXTRINSIC EVIDENCE WILL BE COMFORTABLE TO ME, CORRECT.

MR. KENNEDY: ULTIMATELY YES, YOUR HONOR. AND I KNOW THAT'S WHAT THE COURT WILL DO WHEN IT REACHES THE DELIBERATIVE PROCESS. I RECOGNIZE AS A PRAGMATIC BASIS WITH PEOPLE HERE FROM OUT OF TOWN SITTING IN THE COURTROOM. IF I WERE IN YOUR POSITION, I WOULD BE INCLINED TO SAY "LET'S GET THE EXPERT TESTIMONY OUT OF THE WAY. WE CAN ALWAYS DEAL WITH THE

INTRINSIC RECORD. IT'S HERE FOR ALL TIME."

SO I'M NOT QUARRELING WITH TAKING THE EXTRINSIC EVIDENCE FIRST. BUT DO WE REALLY, I QUESTION, HAVE A FULL DAY OF NEED FOR LAST RESORT TESTIMONY? THIS IS A HIGHLY UNUSUAL CASE IF THAT'S REALLY THE SITUATION. PERHAPS MR. HASLAM COULD ELUCIDATE ON THAT POINT.

MR. HASLAM: WELL, I THINK THE PRAGMATIC ANSWERS IS THE ONE THAT MR. KENNEDY JUST GAVE. THE WITNESSES ARE HERE. THEY HAVE DEPOSED THE WITNESSES, AND EVEN IN THE MOTION SEEKING TO LIMIT OR EXCLUDE, THEY ACKNOWLEDGED THAT THERE WAS SUBJECT MATTER WHICH THEY HAD WHICH WOULD BE PERTINENT.

I'D ALSO LIKE TO POINT OUT THAT MARKMAN WAS THE UNBOTCHED DECISION WHICH SAID THAT THE COURT COULD LISTEN TO EXPERT TESTIMONY TO AID IT IN IT'S INTERPRETIVE PROCESS. IT COULD LISTEN TO OTHER KINDS OF TESTIMONY, AND THE COURT COULD GIVE WEIGHT TO THE VARIOUS ASPECTS OF TESTIMONY AND THAT THE COURT COULD DETERMINE WHICH EVIDENCE, FOR EXAMPLE, OF THE PROSECUTING ATTORNEY OR PERHAPS THE INVENTOR SHOULD BE LOOKED AT WITH CAUTION.

BUT MARKMAN IS THE UNBINDED DECISION. THE VITRONICS CASE IS JUST A PANEL. IN HOECHST V. CELANESE, 78 F.3RD 1575, I'D COMMEND THAT TO THE COURT

WHERE ANOTHER PANEL SPECIFICALLY SAID "BECAUSE JUDGES ARE NOT PEOPLE OF SKILL IN THE ART, THAT THEY SHOULD LISTEN TO TESTIMONY." IT MAY BE CONFIRMATORY OF AN OPINION THAT THE COURT OTHERWISE REACHES. IT MAY BE HELPFUL TO THE PROCESS.

BUT WE SPENT A WHOE DAY YESTERDAY IN A TUTORIAL BECAUSE, WHEN I CAME TO THIS CASE -- AND I STILL HAVE PROBLEMS WITH THE TECHNOLOGY. I DON'T WANT TO SPEAK FOR THE COURT -- BUT THERE ARE ASPECTS HERE ABOUT DIGITAL SIGNATURES, WHAT IT MEANS TO PROVIDE SECURE COMMUNICATIONS WITH COMPUTATIONAL INFEASIBLENESS. ALL OF WHICH THINGS ARE TERMS THAT MAY OR MAY NOT HAVE MEANING IN THE ART, THAT MAY OR MAY NOT BE DEFINED IF SPECIFICATION. BUT UNTIL YOU HAVE HEARD TESTIMONY TO HELP YOU THROUGH WHAT THEY CALL THE INTRINSIC EVIDENCE, IT SEEMS TO ME --

THE COURT: THEY WEREN'T SWORN. IT WAS ARGUMENT.

MR. HASLAM: THAT'S TRUE.

THE COURT: THE PRESENTATION WAS ARGUMENT, AND I WAS ACQUAINTED WITH THE GENERALNESS OF HOW IT FUNCTIONS. I WASN'T REALLY CONCERNED ABOUT THE DETAILS OF THE MATHEMATICAL FORMULA.

MR. HASLAM: AND THAT MAY BE IMPORTANT IN INTERPRETING THESE CLAIMS. AND IT SEEMS TO ME THAT

LISTENING TO THE TESTIMONY THIS COURT, AS I THINK MR. KENNEDY SAID YESTERDAY AT A BENCH TRIAL, COURTS ARE FREQUENTLY PRESENTED WITH EVIDENCE WHICH THEY TAKE IN AND ULTIMATELY GIVE IT THE WAY TO WHICH IT'S ENTITLED OR EXCLUDE IT ALL TOGETHER IF IT'S NOT.

I WOULD THINK IN SOMETHING LIKE THIS, I DON'T THINK IT'S AS ANOMALOUS AS MR. KENNEDY SAYS. I BELIEVE JUDGE WHITE, FOR EXAMPLE, FREQUENTLY SCHEDULES MARKMAN HEARINGS IN WHICH HE LISTENS TO TESTIMONY.

THIS IS NOT A LAWYER HERE TO TELL YOU WHAT THE CLAIMS ARE, AND IF HE STRAYS INTO THAT, YOU ARE PERFECTLY CAPABLE OF IGNORING IT, WHEN YOU GET DOWN TO REVIEWING THE EVIDENCE, AND DECIDING THIS IS NOT TESTIMONY THAT IS TESTIMONY ABOUT WHAT THESE TERMS MAY OR MAY NOT MEAN IN THE ART BUT IS REALLY TRYING TO TELL YOU WHAT YOUR JOB IS.

I HAVE A VAST AMOUNT OF CONFIDENCE IN THE COURT'S ABILITY TO DO THAT TASK AND TO TRY TO PARSE THIS RIGHT NOW AT THIS STAGE IS I THINK NOTHING BUT A CLEVER, WELL-ORGANIZED TACTICAL PLOY TO CHOP UP THE TESTIMONY. WE'RE WASTING MORE TIME ARGUING ABOUT IT THAN JUST PUTTING THEM ON AND ASKING THEM THE QUESTIONS, AND THEY CAN CROSS-EXAMINE THEM. THEY ARE FULLY PREPARED TO CROSS-EXAMINE THEM.

AS A MATTER OF FACT, THEY CITED A TREMENDOUS

AMOUNT OF HIS TESTIMONY TO YOU IN THEIR JURY INSTRUCTION. IT SEEMS TO ME WHAT'S SAUCE FOR THE GOOSE IS SAUCE FOR THE GANDER. LET'S HEAR IT FROM THE HORSE'S MOUTH.

THE COURT: OKAY. WE SHALL ACCOMPLISH THAT WITHIN THE TIME SET ASIDE FOR THIS.

MR. HASLAM: I BELIEVE WE CAN.

MR. KENNEDY: VERY BRIEFLY, YOUR HONOR, OBVIOUSLY, THE REASON WE HELD THE TUTORIAL YESTERDAY WAS ANY HUMAN BEING IS ENTITLED TO SOME KIND OF AN EXPLANATION BEFORE BEING ASKED TO RULE ON MATTERS OF THIS COMPLEXITY.

BUT THE QUESTION FOR TODAY IS WHAT PARTICULAR WORDS, WHAT PARTICULAR LANGUAGE IN THE PATENT CAN'T BE INTERPRETED FROM EITHER THE INTRINSIC RECORD OR FROM DICTIONARIES AND LEGAL METHODS. SURELY MR. HASLAM HAS HIS DIRECT EXAMINATION READY TO GO AND OUGHT TO BE ABLE TO PROVIDE AN ILLUSTRATION. I CAN'T IMAGINE WHY HE CAN'T PROVIDE US AHEAD OF TIME WITH A LIST OF THOSE WORDS THAT HE FEELS REALLY REQUIRE LAST RESORT TESTIMONY FROM DR. KONHEIM. I PREDICT, IF WE DON'T GET THAT TO BEGIN WITH, WE ARE GOING TO QUICKLY BE FALLING INTO DR. KONHEIM TELLING THE COURT HOW THE COURT OUGHT TO INTERPRET THE CLAIMS.

AND WITH ALL RESPECT TO DR. KONHEIM, HE'S NOT

A LAWYER. HE'S NOT A JUDGE, AND THAT'S NOT ANY EXPERT'S ROLE, BUT IT'S YOUR HONOR'S PREFERENCE. BUT I THINK IF WE DON'T GET SOME GROUND RULES, WE'RE QUICKLY GOING TO FIND WE'RE WASTING A LOT OF TIME ON A LOT INADMISSABLE AND INCONSEQUENTIAL EVIDENCE. I'M PREPARED TO SUBMIT IT, YOUR HONOR.

THE COURT: WELL, IF WE START WITH THE INTRINSIC EVIDENCE, START OPENING THE CLAIMS AND THEN DISCUSS THE CLAIMS, WHAT THEY MEAN AND SO FORTH. BUT THAT WILL BE BY COUNSEL OR BY WITNESSES, I GUESS WOULD BE BY WITNESSES.

MR. HASLAM: AS TO WHAT SOME OF THE TERMS IN THE CLAIM MEAN, THAT'S WHAT I INTEND TO HAVE MR. KONHEIM TESTIFY TO. I THINK I AM RATHER STRUCK WITH MR. KENNEDY'S SUGGESTION THAT WE SHOULD HAVE PROVIDED THEM WITH A COPY OF OUR DIRECT EXAMINATION OR SOMETHING OF THAT NATURE BEFOREHAND GIVEN THEIR UNWILLINGNESS TO TELL US WHO THEY WERE GOING TO CALL.

IT SEEMS TO ME WE ARE TAKING PRECIOUS TIME WHICH MR. KENNEDY IS CONCERNED ABOUT WASTING ARGUING ABOUT QUESTIONS WHICH HAVEN'T YET BEEN ASKED, AND WHICH I THINK THE COURT IS MORE THAN CAPABLE OF EITHER STOPPING ON THE SPOT OR WHEN IT READS THE RECORDS ALONG WITH THE VOLUMINOUS SUBMISSIONS THAT HAVE BEEN MADE CAN DETERMINE WHETHER PROFESSOR KONHEIM IS

STRAIGHT OVER THE LINE AND WHAT WEIGHT TO GIVE IT.

THE COURT: WELL, I THINK TO BENEFIT FROM THE TESTIMONY, I'M THE ONE THAT MAKES THE DECISION, AND I CAN ACCEPT OR EXCLUDE WHAT I THINK DIRECTLY OR INDIRECTLY IS PERTINENT.

MR. HASLAM: IT HAPPENS ALL THE TIME IN A BENCH TRIAL.

THE COURT: I'M NOT CONCERNED ABOUT HEARING TESTIMONY. I'M NOT BOUND BY IT. I'M NOT BOUND BY DEFINITIONS IN DICTIONARIES.

MR. HASLAM: RIGHT. AS THE LUBRIZOL CASE SUGGESTS, IT IS THE COURT'S OBLIGATION TO CONSTRUE THE CLAIMS. THE PARTIES ARGUMENTS MAY ASSIST IT, BUT THE COURT ISN'T BOUND TO COME UP WITH AN INTERPRETATION PROCTORED BY ANY OF THE PARTIES IF IT BELIEVES THAT THAT IS NOT THE CORRECT INTERPRETATION OF THE CLAIM.

THE COURT: IF THERE IS ANY TESTIMONY OFFERED BY AN EXPERT THAT THE OTHER SIDE OBJECTS TO, THEY CAN MAKE THE OBJECTION AT THAT TIME, AND WE CAN DISCUSS IT.

MR. HASLAM: THAT'S FINE WITH ME.

THE COURT: WE'LL PROCEED ON THAT BASIS.

MR. HASLAM: I DON'T MEAN TO INTERRUPT THE FLOW. I WOULD LIKE TO MARK THE INITIAL FOUR EXHIBITS. A COPY OF AN ARTICLE "NEW DIRECTIONS IN

CRYPTOGRAPHY." IT'S AN I TRIPLE E TRANSACTION ON INFORMATION THEORY NUMBER SIX, NOVEMBER 1976. A COPY OF THAT IS IN THE PROSECUTION HISTORY WHICH WAS MARKED AS DEPOSITION EXHIBIT 16, BUT THE COPY IN THERE HAS BEEN REDUCED. SO I'D LIKE TO MARK A NEW COPY WHICH I THINK IS MORE LEGIBLE.

THE COURT: PLEASE DO.

MR. HASLAM: AS I'VE SAID, WE'VE MARKED THAT AS EXHIBIT 1000. I'D LIKE TO MARK NEXT ARTICLE ENTITLED "MULTIUSER CRYPTOGRAPHIC TECHNIQUES." AGAIN, THIS IS AN ARTICLE WHICH IS IN THE PROSECUTION HISTORY BUT AGAIN IS REDUCED. SO I'D LIKE TO MARK A MORE LEGIBLE COPY. THIS HAS BEEN MARKED AS EXHIBIT 1001.

THE COURT: OKAY.

MR. HASLAM: NEXT I'D LIKE TO HAVE MARKED AS EXHIBIT 1003 AN ARTICLE ENTITLED "HIDING INFORMATION AND DIGITAL SIGNATURES IN TRAP DOOR KNAPSACKS" BY RALPH MERKLE AND MARTIN HELLMAN. THAT'S BEEN MARKED AS EXHIBIT 1003.

FINALLY, I'D LIKE TO MARK AS EXHIBIT 1004 AN ARTICLE ENTITLED "PRIVACY AND AUTHENTICATION AN INTRODUCTION TO CRYPTOGRAPHY" BY WHITFIELD DIFFIE AND MARTIN HELLMAN. IT'S A PAPER OF THE I TRIPLE E AND IS DATED MARCH 1979. THAT WAS MARKED AS EXHIBIT 1004.

AT THIS TIME I'D LIKE TO CALL PROFESSOR ALAN

KONHEIM TO THE STAND.

THE CLERK: RAISE YOUR RIGHT HAND, PLEASE.

ALAN G. KONHEIM

CALLED AS A WITNESS ON BEHALF OF THE PLAINTIFFS, FIRST BEING DULY SWORN, TESTIFIED AS FOLLOWS:

THE WITNESS: I DO.

THE CLERK: BE SEATED.

PLEASE STATE YOUR FULL NAME AND SPELL YOUR LAST NAME TO THE COURT.

THE WITNESS: ALAN KONHEIM, K-O-N-H-E-I-M.

THE CLERK: WHAT IS YOUR OCCUPATION, SIR?

THE WITNESS: I'M A PROFESSOR IN THE DEPARTMENT OF COMPUTER SCIENCE IN THE UNIVERSITY OF CALIFORNIA AT SANTA BARBARA.

THE CLERK: THANK YOU.

DIRECT EXAMINATION

MR. HASLAM: YOUR HONOR, I'M NOT SURE WHAT YOUR PREFERENCE IS AS TO APPROACHING THE WITNESS.

THE COURT: YOU MAY APPROACH THE WITNESS, AND I'D LIKE YOU TO CROSS-EXAMINE FROM THERE, BUT YOU CAN GIVE THE DOCUMENTS.

BY MR. HASLAM: Q. PROFESSOR KONHEIM, WHAT I'D LIKE TO DO IS GIVE YOU THE COPIES OF THE EXHIBITS I JUST MARKED. I THINK YOU JUST TOLD US WHERE YOU WORK. HOW LONG HAVE YOU BEEN TEACHING AT THE

UNIVERSITY OF CALIFORNIA IN SANTA BARBARA?
A. I'VE BEEN TEACHING 14 YEARS.
Q. THAT'S SINCE ABOUT 1982 THEN?
A. JULY 1, 1982.
Q. WHAT COURSES DO YOU TEACH?
A. I TEACH FOUR COURSES DURING THE YEAR WHICH CONSIST OF THREE QUARTERS. THE FOURTH QUARTER I TEACH A COURSE IN COMPUTER COMPUTATION. IN THE WINTER QUARTER, I TEACH A COURSE IN ASSEMBLY LANGUAGE, AND IN THE SPRING QUARTER, I TEACH TWO COURSES -- A GRADUATE COURSE IN COMPUTER COMMUNICATION AND A COURSE IN CRYPTOGRAPHY.
Q. WHAT DOES THE COMPUTER NETWORK COURSE COVER? WHAT TOPICS?
A. THE COMPUTER NETWORK COURSE DESCRIBES WHAT SORT OF FACILITIES YOU HAVE TO PROVIDE IN ORDER FOR -- THEY HAVE TO BE MACHINE TO MACHINE COMMUNICATION. PROTOCOLS, THE OSI-7 MODEL, ERROR CORRECTING CODES, COMPUTER SECURITY ROUTING, AND ALL OF THE BASIC OPERATIONS THAT ARE REQUIRED IN COMMUNICATION.
Q. I BELIEVE YOU ALSO SAID YOU TEACH A COURSE IN CRYPTOGRAPHY. CAN YOU GIVE US A GENERAL IDEA OF THE KINDS OF THINGS YOU TEACH IN THAT COURSE.
A. YES. THE COURSE IN CRYPTOGRAPHY DEALS WITH THE MATHMATICAL METHODS TO BREAK SYSTEMS. FIRST OF ALL,

IT BEGINS WITH AN OVERVIEW OF CRYPTOGRAPHY, THE GOAL OF CRYPTOGRAPHY, AND IT'S SCIENCE IS THE LEXICON SIX CRYPTOGRAPHY BUT THEN IMMEDIATELY BEGINS TO EXAMINE THE QUESTION OF THE STRENGTH OF CRYPTOGRAPHIC SYSTEMS, HOW YOU GO ABOUT BREAKING A SYSTEM. IT BEGINS WITH SYSTEMS IN THE 16TH CENTURY AND GOES UP TO SYSTEMS IN THE 20TH CENTURY.

Q. AND FOR HOW LONG HAVE YOU TAUGHT A COURSE IN CRYPTOGRAPHY?

A. WELL, I'VE TAUGHT IT WHILE AT U.C.S.B FOR 14 YEARS, BUT I TAUGHT IT -- I BELIEVE I STARTED TO TEACH CRYPTOGRAPHY BEFORE THAT. I MAY HAVE TAUGHT IT AT N.Y.U. ONE YEAR. I THINK I TAUGHT IT INTERNALLY WITHIN I.B.M. FOR SEVEN YEARS.

Q. BY THE WAY, DO YOU -- DOES YOUR COURSE COVER ANY ASPECTS OF CRYPTOGRAPHY RELATED TO TRAP DOOR KNAPSACK?

A. YES, I DESCRIBED THE TRAP DOOR KNAPSACK PROBLEMS, AND I GIVE A HOMEWORK PROBLEM FOR STUDENTS AND ANALYZE THE KNAPSACK PROBLEMS. I DESCRIBED THE RSA ALGORITHM. OF COURSE FOR THAT, THERE IS NO VIABLE METHOD FOR BREAKING THE SYSTEM. SO IT IS MERELY A DESCRIPTIVE HOMEWORK PROBLEM.

Q. IS YOUR COURSE IN CRYPTOGRAPHY SIMILAR TO OTHERS WHICH YOU'RE AWARE?

A. WELL, I'M NOT SURE HOW MANY COURSES ARE DEVOTED IN

THE UNITED STATES SOLELY TO CRYPTOGRAPHY. I KNOW THERE IS ONE GIVEN IN KING COLLEGE IN NEW JERSEY BY SOMEONE WHO IS A FORMER GOVERNMENT EMPLOYEE.

AT ONE TIME, I LOOKED AROUND BECAUSE I WAS ASKED TO DO SO BY SOMEONE AT THE UNIVERSITY. I DON'T THINK THERE ARE MANY COURSES. MANY COURSES TODAY INCLUDE WITHIN THE MATERIAL COVERED SOME ASPECT OF CRYPTOGRAPHY. BUT AS FAR AS I KNOW, THERE ARE NOT MANY COURSES THAT ARE DEVOTED SUBSTATIALLY OR ENTIRELY TO CRYPTOGRAPHY.

Q. HAVE YOU WRITTEN ANYTHING IN THE FIELD OF CRYPTOGRAPHY?

A. YES. AS PART OF MY LEARNING PROCESS THAT STARTED IN 1967, I WROTE A SET OF NOTES ON CRYPTOGRAPHY THAT WAS THE BASIS OF A BOOK THAT I PUBLISHED IN 1980 CALLED "CRYPTOGRAPHY OF PRIMER." IT WAS PUBLISHED BY JOHN WILEY. AND IN ADDITION I'VE WRITTEN FROM TIME TO TIME PAPERS ON CRYPTOGRAPHY.

Q. LET ME BACK UP NOW. CAN YOU JUST GIVE US A BRIEF OVERVIEW OF YOUR EDUCATIONAL BACKGROUND.

THE COURT: I THINK WE HEARD THAT YESTERDAY. I THINK YOU CAN PROCEED ABOUT THE QUESTIONS OF THE COURSE TODAY. I'VE CERTIFIED HE'S AN EXPERT, AND I RECOGNIZE HE'S AN EXPERT. I THINK THAT'S SUFFICIENT FOR HIM TO GO FORWARD.

MR. HASLAM: I UNDERSTAND, YOUR HONOR. IF I CAN JUST ASK, BECAUSE IT DOES LAY A CONTEXT FOR SOME SUBSEQUENT TESTIMONY, IF I CAN JUST ASK THE WITNESS TO BRIEFLY COVER SOME OF THE THINGS HE DID IN HIS WORK EXPERIENCE.

THE COURT: OKAY.

BY MR. HASLAM: Q. TAKING THE COURT'S ADMONITION INTO ACCOUNT, CAN YOU GIVE US A BRIEF OVERVIEW OF YOUR WORK EXPERIENCE AT I.B.M.

A. YES. WHEN I JOINED I.B.M. IN 1960, I JOINED IN THE MATHEMATICS DEPARTMENT. MY FIRST RESPONSIBILITIES WERE IN THE EVALUATION OF VARIOUS SCHEMES FOR DOING PATENT RECOGNITION. AND THEN AT THE ADVICE OF THE PROFESSOR WHO WAS ADVISING ME ON MY POST GRADUATE EDUCATION, I BEGAN TO WORK IN THE AREA OF COMPUTER NETWORKS AND PERFORMANCE EVALUATION.

THE COURT: 1960 YOU SAY?

THE WITNESS: I BEGAN TO WORK IN 1960, YOUR HONOR, WHEN I GRADUATED FROM CORNELL.

THE COURT: UPSTATE NEW YORK?

THE WITNESS: YES, UPSTATE NEW YORK.

THE COURT: WHERE IS IT?

THE WITNESS: ITHACA, NEW YORK. IN 1967 I HAD A NEW RESPONSIBILITY AND CONTINUED ESSENTIALLY LARGELY UNTIL I LEFT I.B.M. IN 1982. I.B.M. HAD

DECIDED THAT IT WANTED TO OFFER ITS CUSTOMERS A PRODUCT WHICH WOULD PROTECT THEIR INFORMATION, INFORMATION NOT ONLY TRANSMITTED BETWEEN MACHINES, BUT INFORMATION STORED IN MEMORY ON A MACHINE.

SO I.B.M. -- IN FACT, IT ENGAGED THE SERVICES OF SOMEONE WHO HAD FLED GERMANY IN THE 1930'S, AND IT HAD CONTINUING INTEREST IN CRYPTOGRAPHY. HE BEGAN TO WORK, AND I HEADED AN EFFORT TO DEVELOP AN I.B.M. PRODUCT IN THIS AREA. THIS ALGORITHM WAS CALLED LUCIFER, AND THIS ALGORITHM WOULD TAKE EIGHT ALPHABETIC CHARACTERS, THAT IS, TEXT IN GROUPS OF EIGHT AND WOULD ENCIPHER IN GROUPS OF EIGHT.

IT'S WHAT WAS REFERRED TO IN CRYPTOGRAPHY AS A BLOCK CIPHER. ACTUALLY AT THE SAME TIME THAT I.B.M. BEGAN THIS, A CUSTOMER APPROACHED I.B.M. AND ASKED IF IT WOULD DESIGN SECURITY FEATURES FOR A CASH ASSURANCE SYSTEM MUCH LIKE THAT WHAT APPEARS OVER THE UNITED STATES NOW. THE CONCERNED WAS LLOYDS BANKING OF LONDON. IT INVOLVED PUTTING A CRYPTOGRAPHIC FEATURE WITHIN THE A.T.M. SYSTEM TO DESIGN THE PROTOCOL FOR HOW THE CUSTOMER WOULD INTERACT WITH THE SYSTEM, AND IT INVOLVED A CRYPTOGRAPHY.

AFTER THE SYSTEM BECAME -- WAS IMPLEMENTED BY THE CUSTOMER, WE ESTABLISHED THE RELATIONSHIP WITH THE UNITED STATES GOVERNMENT, AND I.B.M. DESIGNED ANOTHER

ALGORITHM TO A FOLLOWING ONTO LUCIFER WHICH BECAME THE DATE ENCRYPTION. I WAS INVOLVED FROM '67 ON UNTIL I LEFT I.B.M. IN 1982 WITH VARIOUS ASPECTS OF D.E.S.

Q. WAS D.E.S., THE DATA ENCRYPTION STANDARD, EVER ADOPTED OUTSIDE OF I.B.M.?

A. YES, SOMETIME I THINK IN 1970, THE FEDERAL GOVERNMENT SOLICITED FROM INDUSTRIAL GROUPS FROM EVEN INDIVIDUALS ALGORITHMS TO BE SUBMITTED TO THE NATIONAL BUREAU OF STANDARDS, WHICH HAS SINCE BEEN RENAMED. AND THESE ALGORITHMS WOULD BE EXAMINED, TESTED, CERTIFIED BY THE NATIONAL BUREAU OF STANDARDS, AND ONE OR MORE OF THEM WOULD BE DESIGNATED AS A NATIONAL STANDARD CRYPTOGRAPHICAL GEM. I'M NOT SURE HOW MANY ALGORITHMS WERE SUBMITTED, BUT D.E.S. WAS ONE OF THEM AND CERTIFIED AS A STANDARD IN 1976.

Q. WHEN YOU SAY, "CERTIFIED AS A STANDARD," CAN YOU TELL ME THE PROCESS, AS YOU UNDERSTOOD IT, THAT IT WENT THROUGH PRIOR TO BEING CERTIFIED AS A STANDARD?

A. WELL, I CAN ONLY REALLY GIVE YOU PRECISE INFORMATION ABOUT WHAT I.B.M. DID ALTHOUGH IT'S INFERRED THAT N.B.S. AND ITS AGENT N.S.A. DID THE SAME ACTIVITY. WE STUDIED THE ALGORITHM, AND WE HIRED EXPERTS. FOR EXAMPLE, THERE WAS A VERY DISTINGUISHED PROFESSOR ONIC BERLING FROM THE INSTITUTE FOR ADVANCED STUDY THAT WORKED ON THE ANALYSIS OF THE GERMAN GAHEIM

STRIGER WHICH WAS ONE OF THE PRINCIPAL GERMAN EXPERTS. WE HIRED HIM. WE HIRED OTHER EXPERTS.

THE ENTIRE GROUP OF SIX OR SEVEN PEOPLE BEGAN TO STUDY THE ALGORITHM AND EXAMINE IT IN ALL ASPECTS TO DETERMINE WHETHER THIS ALGORITHM COULD BE CRACKED, WHETHER THERE WAS SOME WAY WITHIN SOME PERIOD OF TIME THAT YOU COULD RECOVER WHAT THE KEY WAS, LEARNED WHAT THE PLAIN TEXT WAS.

N.B.S. THROUGH ITS SOLICITATION ALSO, I THINK, ENGAGED IN THIS PROCESS. N.B.S. HELD TWO WORKSHOPS TO SOLICIT AND ENCOURAGE OUTSIDE COMMENTS ABOUT THE DATA ENCRYPTIONS, AND I KNOW THAT MARTY HELLMAN ATTENDED ONE, AND I ATTENDED ONE. THERE WERE MANY CRITICISMS OF I.B.M. AND MUCH DISCUSSION ABOUT I.B.M.'S D.E.S. ALGORITHM.

AND ULTIMATELY AT THE END OF A PERIOD OF PERHAPS FOUR YEARS, THE NATIONAL BUREAU OF STANDARDS DECIDED IT'S CERTIFIED. IT'S ALSO BEEN RECERTIFIED, I THINK, TWICE AND THERE'S A NEW CERTIFICATION THAT IS COMING UP WITHIN THE NEXT YEAR OR SO.

Q. NOW, I WANT TO TURN TO THE WORK YOU DID IN PREPARATION FOR TESTIFYING HERE TODAY AND FOR THE DECLARATION THAT YOU PROVIDED EARLIER.

HAVE YOU REVIEWED WHAT'S BEEN REFERRED TO AS THE '582 PATENT WHICH I BELIEVE IS EXHIBIT 13?

A. YES, I HAVE.
Q. IN THE BINDERS TO YOUR RIGHT, THERE ARE EXHIBITS. IF YOU COULD LOOK AT EXHIBIT 13.
A. YES, I HAVE REVIEWED '582.
Q. IF YOU LOOK AT EXHIBIT 16, WHICH I BELIEVE IS WHAT'S REFERRED TO AS THE FILE WRAPPER OR PROSECUTION HISTORY OF THE '582 PATENT.
A. YES, I HAVE REVIEWED THIS DOCUMENT.
Q. AND HAVE YOU ALSO REVIEWED ANY ARTICLES OR OTHER LITERATURE ABOUT THE ART OR STATE OF THE ART RELATING TO THE '582 PATENT?
Q. YES, I READ -- I ACTUALLY REREAD A NUMBER OF ARTICLES THAT I HAD READ BEFORE I'D READ THE ARTICLE BY WHITFIELD DIFFIE AND MARTY HELLMAN CALLED "MULTIUSER CRYPTOGRAPHIC TECHNIQUES," AND MAYBE I'VE MISSTATED THE TITLED OF -- "MULTIUSE OF CRYPTOGRAPHIC TECHNIQUES." I READ THEIR PAPER ON "NEW DIRECTIONS IN CRYPTOGRAPHY."

I READ THE PAPER OF MARTY HELLMAN AND RALPH MERKLE ON TRAP DOOR KNAPSACK SYSTEMS, AND I READ THE PAPER BY MARTY HELLMAN AND WHITFIELD DIFFIE, THE PAPER ON "PRIVACY IN AUTHENTICATION AND INTRODUCTION INTO CRYPTOGRAPHY."

Q. NOW, I WANT TO TURN TO TERMS THAT ARE USED IN THIS FIELD. I WANT TO START OFF WITH --

THE COURT: LET'S TAKE A BREAK.

(A RECESS WAS TAKEN.)

MR. HASLAM: Q. WHAT DO YOU UNDERSTAND IS MEANT BY A SECURE CRYPTOGRAPHIC SYSTEM?

A. WELL, A SECURE CRYPTOGRAPHIC SYSTEM IS A SYSTEM THAT'S TO PROVIDE SECRECY WHETHER THAT SECRECY IS GOING TO BE USED TO HIDE INFORMATION OR USED AS PART OF AUTHENTICATION. BUT THE PROCESS IS REALLY DESCRIBED BY ITS TWO ATTRIBUTES, AND THE ATTRIBUTES ARE AS FOLLOWS. IT GUARANTEES TO PROVIDE SECRECY AGAINST ANY AND ALL METHODS THAT PEOPLE CAN BRING TO BEAR AGAINST THE SYSTEM.

THE COURT: FEASIBLE METHOD?

THE WITNESS: FEASIBLE? WELL, IT GUARANTEES IT. WHETHER THE GUARANTEE WILL LAST FOR A YEAR OR FOR A WEEK IS GOING TO DEPEND UPON THE METHODS. SO IN FACT, THE SECOND ATTRIBUTE IS THAT THAT GUARANTEE SHOULD BE FOR AT LEAST SOME TIME.

SO IT SAYS I GUARANTEE THAT THIS INFORMATION WILL BE KEPT SECRET FROM EVERYTHING, EVERYONE. AND SECOND, I GUARANTEE THAT THAT INFORMATION WILL BE KEPT SECRET FOR AT LEAST TWO YEARS. SO THOSE ARE THE TWO ATTRIBUTES. IT DOESN'T TELL YOU HOW TO DO IT. IT ONLY TELLS YOU THE RESULTS OF SECURE COMMUNICATIONS.

THE COURT: SOME DAY THEY'LL GET BACK TO

HANDING THE BRIEFCASE OVER.

THE WITNESS: MAY THAT OR CARRIER PIGEONS.

MR. HASLAM: Q. I BELIEVE THERE WAS SOME DISCUSSION ABOUT THE TIME VALUE OF INFORMATION. IS THAT WITH THE SECOND ATTRIBUTE?

A. YES. I THINK PROFESSOR HELMAN POINTED OUT YESTERDAY THAT IN SOME ENVIRONMENT, FOR EXAMPLE, MILITARY COMMUNICATIONS, THE SECRECY DOESN'T HAVE TO BE MAINTAINED FOR A MILLION YEARS. IT MAY HAVE TO BE MAINTAINED ONLY FOR A MONTH OR FOR TWO MONTHS DEPENDING UPON WHEN THE ACTION IS TO TAKE PLACE.

BUT THEN THERE ARE SOME EXAMPLES WHERE THE SECRECY MUST BE MAINTAINED FOR A MUCH LONGER PERIOD OF TIME. AS I MENTIONED BEFORE, THE WORK FOR LLOYDS BANKING INVOLVES A.T.M.'S. ONE OF THE THINGS THAT YOU HAVE IN AN A.T.M. IS A PERSONAL INFORMATION NUMBER WHICH TOGETHER WITH THE CARD ENABLES YOU TO GET CASH FROM AN UNATTENDED BANKING TERMINAL. THAT PIN HAS GOT TO BE PROTECTED AS LONG AS YOU OWN THE CARD.

SO IT'S GOT TO BE PROTECTED FOR 10'S OF YEARS OR 50 YEARS. MY MEDICAL REPORTS I WANT TO BE PROTECTED AS LONG AS I'M ALIVE. SO DEPENDING UPON WHAT THE APPLICATION IS, THERE HAS TO BE SECRECY MAINTAINED FOR SOME LENGTH OF TIME DEPENDING UPON WHAT THE APPLICATION IS, AND I THINK THAT THAT'S UNDERSTOOD

IN THE BUSINESS OF CRYPTOGRAPHIC SYSTEMS BECAUSE THERE ARE SOME SYSTEMS WHICH WOULD BE VALID FOR CLASSIFIED DATA AND SOME SYSTEMS WHICH WOULD BE DATA FOR TOP SECRET DATA.

SO THEY ARE SUPPOSED TO PROVIDE SECURITY FOR A CERTAIN AMOUNT OF TIME, AND THAT DEPENDS UPON THE INTRINSIC STRENGTH OF THE ALGAMY.

Q. HOW DO CRYPTOGRAPHERS GO ABOUT DETERMINING WHAT YOU JUST REFERRED TO AS THE INTRINSIC STRENGTH OR SECURITY OF A SYSTEM?

A. THE ANSWER IS VERY COMPLICATED.

MR. KENNEDY: YOUR HONOR, IT'S ALSO IRRELEVANT TO INTERPRETATION OF THIS TERM IN THE PATENT.

MR. HASLAM: THE PATENT REFERS TO PROVIDING A METHOD OF SECURE COMMUNICATION, AND IT SEEMS TO ME HOW YOU DETERMINE WHETHER A COMMUNICATION IS SECURE, AND HOW PEOPLE IN THE ART DEFINE THAT TERM, AND HOW THEY DETERMINE IT IS RELEVANT AS TO HOW THE COURT'S GOING TO CONSTRUE WHAT IT MEANS TO HAVE A SYSTEM WHICH PROVIDES SECURE COMMUNICATION.

MR. KENNEDY: IT SOUNDS LIKE AN INVALIDITY ATTACK TO ME, YOUR HONOR. IF THEY ARE CLAIMING THE PATENT IS INVALID AND DOESN'T DO WHAT IT PROMISES, THAT'S AN ISSUE FOR ANOTHER DAY.

THE QUESTION NOW IS WHAT DID THE WORDS IN THE PATENT MEAN, AND WHY ARE THEY NOT DEFINED OTHERWISE SUCH AS THIS MAN TO HAS TO BE GIVING HIS LAST RESORT OPINION?

THE COURT: REPEAT THE QUESTION, PLEASE.

MR. HASLAM: HOW DO CRYPTOGRAPHERS DETERMINE WHETHER A SYSTEM PROVIDES THE SECURE COMMUNICATION WHICH YOU HAVE TESTIFIED IS INTRINSIC OR INHERENT IN ANY SYSTEM.

THE COURT: OBJECTION OVERRULED.

THE WITNESS: THE ANSWER IS THAT PEOPLE STUDY THE SYSTEM. IT IS A GROUP OF PEOPLE, FOR EXAMPLE, WITHIN THE GOVERNMENT, ONE GROUP DESIGNS THE ALGORITHM, ANOTHER GROUP BEGINS TO ATTACK THE ALGORITHM. BASED ON THE EXPERTISE THEY HAVE DEVELOPED OVER A PERIOD OF TIME, THEY BEGIN TO APPLY THAT TO TRY TO FIND THE SOLUTION.

IF THEY DON'T FIND THE SOLUTION, IT DOESN'T MEAN THAT THE SYSTEM IS SECURE. BUT IF THIS IS DONE OVER AN EXTENDED PERIOD OF TIME WITH COMPETENT PEOPLE, THE LESS LIKELY THAT A SOLUTION WILL BE FOUND AND MORE CONFIDENCE THAT YOU GAIN WITHIN THE SYSTEM.

IT'S MUCH LIKE THE SAME AS WHEN YOU TEST A DRUG. YOU TAKE A DRUG. YOU GIVE IT TO A TEST GROUP OF PEOPLE, AND YOU SEE WHETHER THEY GET BETTER OR

WORSE. IF THEY ALL GET BETTER, IT DOESN'T MEAN THAT THE DRUG IS GOING TO MAKE EVERYONE WELL. BUT THE MORE LONGER YOU TEST IT, THE MORE EXPERIENCE YOU HAVE WITH THE DRUG, THE MORE CONFIDENCE YOU GAIN THAT THE DRUG IS GOING TO ACT IN A POSITIVE WAY.

BUT BEFORE YOU DO THAT, YOU NEVER DISTRIBUTE THE DRUG TO PEOPLE. THAT'S THE SORT OF PARADIME THAT THE FDA USES. IT TESTS THE DRUG, SEES THE EFFECT OF THE DRUG ON PEOPLE, AND THEN CERTIFIES THE DRUG AS BEING ACCEPTABLE FOR THE MARKETING WITHIN -- FOR THE GENERAL PUBLIC. THE SAME IS TRUE OF CRYPTOGRAPHY. YOU STUDY THE ALGORITHM, USE THE BEST SKILLS THAT YOU HAVE TO ANALYZE IT, AND WHEN AFTER A REASONABLE PERIOD OF TIME YOU DON'T FIND ANY METHOD OF ANALYSIS, THEN YOU BEGIN TO FEEL CONFIDENT THAT THE ALGORITHM IS GOOD.

THE COURT: WELL, THE GOVERNMENT CERTIFICATE OF APPROVAL THAT WAS GIVEN -- DOES THAT SORT OF VALIDATE THE I.B.M. SYSTEM?

THE WITNESS: YES, THAT IN FACT WAS PART OF THIS CERTIFICATION PROCESS.

THE COURT: A COMPANY CAN'T MARKET A PRODUCT THEY SAY IS SECURE UNLESS IT GETS CERTIFICATION.

THE WITNESS: I'M NOT SURE. WE DON'T INSIST WITHIN THE UNITED STATES THAT THE GOVERNMENT CERTIFY

EVERY CRYPTOGRAPHIC ALGORITHM.

THE COURT: IF THAT'S TRUE, THE UNITED STATES WOULD GIVE UP.

THE WITNESS: IN THE CASE OF D.E.S., THE ALGORITHM WAS TESTED BY THE NATIONAL SECURITY AGENCY OVER A PERIOD OF CERTAINLY THREE OR FOUR YEARS BEFORE THE NATIONAL BUREAU OF STANDARDS SAID "YES, WE DECLARE THAT THIS ALGORITHM IS ADEQUATE FOR PROTECTING YOUR INFORMATION."

THE COURT: BUT THE INDUSTRY DOESN'T HAVE TO GO TO THE GOVERNMENT AGENCY --

THE WITNESS: NO, NO. THE INVENTORS OF '582 DIDN'T GO TO THE NATIONAL BUREAU OF STANDARDS, WEREN'T REQUIRED TO GO TO IT, NOR THE INVENTORS OF THE RSA GO AND SAY, "WE WANT CERTIFICATION THAT THIS ALGORITHM MEETS THE TESTS THAT YOU WILL PUT INTO PLACE TO TELL THE GENERAL PUBLIC THAT IT'S ALL RIGHT TO USE IT." IT WILL GUARANTEE SECRECY FOR YOUR INFORMATION. YOU DON'T HAVE TO DO IT, NOT AT THE PRESENT TIME.

MR. HASLAM: Q. I THINK WE LEARNED YESTERDAY THAT CRYPTOGRAPHY AT LEAST BORROWS A LOT FROM MATHEMATICS; IS THAT CORRECT?

A. YES, I THINK SO.

Q. WHY CAN'T YOU, GIVEN THAT, SIMPLY PROVE MATHEMATICALLY THE SECURITY OF THE SYSTEM?

A. WELL, IT'S JUST NOT POSSIBLE IN GENERAL. THERE IS ONE SYSTEM THAT WAS INVENTED PROBABLY IN THE 1920'S BY JOSEPH MORBER AT U.S. CIGNA CORP. CALLED THE "ONE TIME SYSTEM." IT'S BEEN USED FOR THE PAST 70 YEARS, AND IT ABSOLUTELY UNEQUIVOCALLY GUARANTEES THE SECURITY OF INFORMATION.

IN SPITE OF THAT, YOUR HONOR, THE RUSSIANS, WHO ALSO USED IT, MADE A MISTAKE DURING THE SECOND WORLD WAR IN ITS USE NOT IN THE ALGORITHM BUT THE WAY THEY USED IT, AND IT LED TO A TREMENDOUS DISCOVERY BY THE UNITED STATES OF RUSSIAN INTELLIGENCE.

BUT THAT SYSTEM IF USED CORRECTLY ABSOLUTELY GUARANTEES. IT CAN BE MATHEMATICALLY PROVED. BUT EXCEPT FOR THAT SYSTEM, YOU CANNOT PROVE MATHEMATICALLY THAT A SYSTEM WILL GIVE COMPLETE SECURITY BECAUSE IT'S ONLY A FINITE NUMBER OF KEYS THAT YOU HAVE TO TEST. AND SO IF YOU TEST ALL KEYS, CERTAINLY YOU WILL FIND SOME ONE KEY WHICH WILL GIVE YOU READABLE PLAIN TEXT.

AND WHEN YOU SEE THAT, YOU CAN ALWAYS SAY THAT'S THE KEY WHICH THE USER IS USING. SO I INTERCEPT SOME CIPHER TEXT THAT MARTY HELLMAN HAS TRANSMITTED OR PRESIDENT ROOSEVELT HAS TRANSMITTED TO GENERAL EISENHOWER. I TRY ALL POSSIBLE KEYS, AND ONE OF THEM IS GOING TO GIVE ME SOMETHING THAT I CAN

READ.

SO THEREFORE, I CAN'T PROVE MATHEMATICALLY THAT YOU CAN'T DO IT BECAUSE I'VE SHOWED HOW TO DO IT. THE TROUBLE IS, THOSE SYSTEMS MAY STILL BE SECURED IF I CAN'T DO THE ACT THAT I JUST DESCRIBED TO YOU. THAT IS, I CAN'T TEST ALL KEYS BECAUSE THERE ARE TOO MANY KEYS.

IN THIS CASE INSTEAD OF PROVIDING WHAT IN THE FIRST CASE IS CALLED UNCONDITIONAL SECURITY, AN ABSOLUTE GUARANTEE, WE PROVIDE SOMETHING WHICH IS CALLED A COMPUTATIONAL GUARANTEE OF SECURITY. THAT IS, YOU JUST CAN'T CARRY OUT THE PHYSICAL ACT OF TESTING ALL THESE, BUT YOU CAN'T MATHEMATICALLY PROVE THAT IT'S SECURE BECAUSE IF YOU COULD IN FACT TEST ALL THE KEYS AND FIND THE CORRECT KEY.

BUT NEVERTHELESS OUR SYSTEMS MAY BE CERTIFIED IF THE VERY ACT OF DOING THIS THING IS IMPOSSIBLE TO DO, THEN WE'RE CONFIDENT IF THE ONLY WAY OF DOING THIS IS TRYING ALL THE KEYS, AND IF YOU CAN TRY ALL THE KEYS, THEN IT IS SECURE.

Q. DID THE INVENTORS OF THE '582 PATENT PROVE THAT THE TRAP DOOR KNAPSACK SYSTEMS WHICH WERE DISCLOSED THERE WERE SECURE OR PROVIDED A MEANS OF SECURE COMMUNICATION?

A. WELL, THEY WRITE IN THE PATENT THAT THEY ARE

DESCRIBING A SECURE COMMUNICATIONS SYSTEM, INDICATED IN THE PATENT IN ONE OF THE CLAIMS, IN CLAIM ONE, THAT THE PROCESS OF BREAKING THE SYSTEM IS COMPUTATIONALLY INFEASIBLE. THAT'S WHAT WE'VE BEEN DESCRIBING AS NEEDING THE TEST FOR CERTIFICATION. BUT THEY DID NOT ACTUALLY PARTICIPATE IN ANY CERTIFICATION ACTION AT THE TIME THE PATENT WAS FILED.

AUTHORS DID SAY IN THERE THEY CHALLENGED PEOPLE. THEY WANTED PEOPLE TO STUDY THE PROBLEM BECAUSE THEY WANTED TO DETERMINE WHETHER THIS ENCRYPTION SYSTEM WAS COMPUTATIONALLY INFEASIBLE TO BREAK AS INDICATED. BUT AT THE TIME THE PATENT WAS ISSUED -- AT THE TIME THE PATENT WAS FILED, IT'S CERTAINLY NOT THE CASE THAT THEY SUBMITTED THIS TO A CERTIFICATION PROCESS.

Q. JUST SO I'M CLEAR, DID THEY MATHEMATICALLY PROVE -- IS THIS ONE OF THOSE ALGORITHMS WHICH WAS MATHEMATICALLY PROVED TO PROVIDE A METHOD OF SECURE COMMUNICATION?

A. NO, NOT AT ALL.

Q. SO THIS WAS A SYSTEM, THEN, WHERE SOME SORT OF CERTIFICATION PROCESS WOULD BE NECESSARY TO DETERMINE WHETHER IT PROVIDED A METHOD OF SECURE COMMUNICATION?

A. THAT'S CORRECT. IT REQUIRED SOME TYPE OF CERTIFICATION.

Q. DO YOU KNOW OR HAVE ANY BASIS FOR TELLING US

WHETHER YOUR OPINION THAT THE SECURITY OF THIS, THE TRAP DOOR KNAPSACK CRYPTOGRAPHIC SYSTEM, HAD TO BE CERTIFIED SINCE IT WASN'T PROVEN TO PROVIDE A METHOD OF SECURE COMMUNICATION?

A. WELL, THE AUTHORS THEMSELVES IN ONE OF THEIR ARTICLES, THE ARTICLE BY PROFESSOR HELLMAN AND RALPH MERKLE WHICH I BELIEVE IS EXHIBIT 1003.

Q. CAN YOU GIVE US THE TITLE OF THAT?

A. THE TITLE OF THAT IS "HIDING INFORMATION AND DIGITAL SIGNATURES IN TRAP DOOR KNAPSACKS." THEY WROTE ON PAGE 529 "WE HAVE NOT PROVED THAT IT IS COMPUTATIONALLY DIFFICULT FOR AN OPPONENT WHO DOES NOT KNOW THE TRAP DOOR TO SOLVE THE PROBLEM." THEY GO ON TO SAY IN --

THE COURT: WHERE IS THAT?

THE WITHESS: IT'S ON PAGE 529, THE SECOND COLUMN, YOUR HONOR, THE SECOND COLUMN.

THE COURT: WHAT'S THE HEADING OF THE PARAGRAPH?

THE WITNESS: THE HEADING OF THE PARAGRAPH IS "VII DISCUSSION." THE SECOND PARAGRAPH BEGINS WITH "WE HAVE NOT PROVED THAT IT IS" --

THE COURT: MINE DOESN'T HAVE ANY PAGE NUMBERS ON IT.

THE WITNESS: CAN I GIVE YOU MINE, YOUR HONOR?

MR. HASLAM: IN THE UPPER RIGHT-HAND CORNER I BELIEVE, 529. IT SHOULD BE THE SECOND TO LAST PAGE IN THE EXHIBIT. THERE'S A "VII DISCUSSION."

THE COURT: ALL RIGHT.

MR. KENNEDY: YOUR HONOR, I'D OBJECT TO MOVE TO STRIKE ON THE GROUNDS THAT IT SOUNDS AS THOUGH THEY ARE TRYING TO SHOW NOW THE PATENT IS NONENABLING IN SAYING THE TRAP DOOR KNAPSACK SIMPLY DOESN'T DO WHAT THE PATENT CLAIMED. THAT MIGHT BE A NICE ATTACK BEFORE THE PATENT OFFICE. IT MIGHT HAVE SOME POINT IN THESE PROCEEDINGS, BUT SUBMIT IT HAS NOTHING TO DO WITH MARKMAN CLAIMS CONSTRUCTION. AT BEST IT SEEMS TO BE AN ATTACK ON ENABLING.

MR. HASLAM: I BELIEVE THAT THE OBJECTION MR. KENNEDY MADE BEFORE WAS OF THE SAME THING WHICH SOUNDS LIKE IT'S GOING TO VALIDITY, BUT REALLY IF THE PATENT DIDN'T DO WHAT IT PROMISED AND WHAT WE'RE HERE TO DO IS WHAT IT SAYS IT CAN DO AND ONCE WE KNOW WHAT THE TEST IS, THEN WE CAN GO LOOK AND SEE IF IT DOES IT.

BUT YOU HAVE TO CONSTRUE THE CLAIMS FOR INFRINGEMENT THE SAME AS YOU DO FOR VALIDITY. AND YOU HAVE TO CONSTRUE THE CLAIMS, THEN WE KNOW THE TARGET THAT THESE INVENTORS SET UP AND WHETHER WHAT THEY DISCLOSED MET THAT TARGET. BUT TO SAY THAT WE'RE

PUTTING THE CART BEFORE THE HORSE IS WRONG. YOU HAVE TO CONSTRUE THE CLAIMS THE SAME FOR VALIDITY AND INFRINGEMENT.

ONCE WE KNOW WHAT THEY PROMISED, ONCE WE KNOW WHAT THE TERM TO PROVIDE SECURE COMMUNICATION MEANS, THEN WE CAN DETERMINE WHETHER THEY DID IT OR NOT.

MR. KENNEDY: YOUR HONOR, THAT'S NOT WHAT THE LAST LINE OF QUESTIONS HAS GONE TO. THE LAST LINE OF QUESTIONS RELATED TO DID THE PARTICULAR PREFERRED EMBODIMENT, THE TRAP DOOR KNAPSACK, IN FACT ACCOMPLISH WHAT THE PATENT SET OUT TO DO.

THE COURT: I DON'T THINK HE SAID THAT.

MR. HASLAM: JUST TO REPEAT IF THERE IS ANY MISCOMMUNICATION, THE QUESTION WAS --

THE COURT: LET'S HEAR THE QUESTION AGAIN.

MR. HASLAM: COULD WE HAVE THE QUESTION READ BACK OR WOULD YOU LIKE ME TO RESTATE IT? I'LL RESTATE IT.

THE COURT: FINE.

MR. HASLAM: Q. IS THERE ANYTHING WHICH YOU'RE AWARE IN THE ART THAT CONFIRMS OR DOESN'T CONFIRM YOUR VIEW THAT THE SECURITY OF A CRYPTOGRAPHIC SYSTEM AND ITS ABILITY TO PROVIDE A SECURE COMMUNICATION MUST BE CERTIFIED WHEN IT IS NOT MATHEMATICALLY PROVEN?

A. AND MY ANSWER TO THE QUESTION REMAINS YES.

THE COURT: CERTIFIED BY WHO.

THE WITNESS: CERTIFIED BY PEOPLE IN THE CRYPTOGRAPHIC COMMUNITY WHO WORK IN THIS AREA THAT THERE IS NO NATIONAL --

THE COURT: IF IT'S JUST THE USERS, IT'S NOT A GOVERNMENT CERTIFICATION.

THE WITNESS: THAT'S RIGHT. IT'S NOT A GOVERNMENT CERTIFICATION. IT'S A CERTIFICATION BY PEOPLE WORKING IN THE AREA OF CRYPTOGRAPHY. THERE IS NO FORMAL PROCESS BY WHICH CERTIFICATION CAN BE ACHIEVED. THAT IS, I CAN'T GO TO THE FDA AND SAY, "CERTIFY THIS CRYPTOGRAPHIC ALGORITHM." THAT'S NOT WITHIN THEIR CHARTER, BUT I CAN PUBLISH THIS ALGORITHM AND CHALLENGE PEOPLE IN THE CRYPTOGRAPHIC COMMUNITY TO STUDY THE ALGORITHM.

AND WHEN THEY HAVE STUDIED THE ALGORITHM TO SAY, NO, I'M NOT DOING AN ANALYSIS, IF A NUMBER OF YEARS GO BY WITH NO BREAKS OF THE SYSTEM, THE LONGER THE PERIOD THE MORE CONFIDENT YOU ARE. BUT THE QUESTION THAT MR. HASLAM IS ASKING ME, IS THERE ANYTHING THAT SUGGESTS THAT THE AUTHORS WERE AWARE OF THAT PROCESS, WHATEVER CERTIFICATION IS.

THE COURT: THAT'S THE LONG ANSWER TO A SHORT QUESTION.

THE WITNESS: I'LL TRY TO BE MORE BRIEF. ON PAGE 529 --

THE COURT: WHAT PAGE?

THE WITNESS: 529 ON THE RIGHT-HAND COLUMN.

THE COURT: DISCUSSION. IT SAYS WE HAVE SHOWN RESPONSE TO KNAPSACK --

THE WITNESS: MAY I DIRECT YOUR ATTENTION TO THE LAST THREE LINES, SECOND PARAGRAPH OF THAT SECTION.

THE COURT: "FAITH IN THE SECURITY OF THESE SYSTEMS MUST THEREFORE REST ON INTUITION AND THE FAILURE OF CONCERTED ATTEMPTS TO BREAK THEM."

THE WITNESS: AND THAT'S THE POINT.

THE COURT: IT DOESN'T SAY "GUARANTEE"?

THE WITNESS: IT DOESN'T OFFER GUARANTEE. THIS IS OFFERING SECURITY, DEPENDS UPON THE ABILITY OF PEOPLE TO STUDY THE SYSTEM AND TO SEE WHETHER THEY HAVE CRACKED THE SYSTEM.

THE COURT: THE SECOND PARAGRAPH SAYS, "WE HAVE NOT PROVED THAT IT IS COMPUTATIONALLY DIFFICULT FOR AN OPPONENT WHO DOES NOT KNOW THE TRAP INFORMATION TO SOLVE THE PROBLEM. CONCLUSIVE PROOF OF SECURE COMMUNICATION ARE NOT YET AVAILABLE FOR NORMAL CRYPTOGRAPHIC SYSTEMS. EVEN THE KNAPSACK PROBLEM HAS NOT BEEN PROVED DIFFICULT TO SOLVE."

THE WITNESS: THE INVENTORS ADMIT THAT IT'S -- THAT IN CONTRARY TO WHAT THEY CLAIM THEMSELVES IN CLAIM ONE, THEY CLAIM THAT IT IS COMPUTATIONALLY DIFFICULT. AND IN THIS ARTICLE OVER HERE WHICH DEALS WITH THE SAME SYSTEM, THEY NOW CONTRADICT THEMSELVES. THEY ARE SAYING THEY HAVEN'T PROVED IT.

MR. KENNEDY: YOUR HONOR, OBJECT AND MOVE TO STRIKE. NOW HE HAS JUST TESTIFIED THE PATENT IS NOT --

THE COURT: I'LL STRIKE THAT PORTION. I ASKED A QUESTION AND GOT A LONGER ANSWER THAN I WAS SEEKING. THIS IS DISCUSSION IN AN ARTICLE BY THE INVENTORS OF THIS INVENTION AND SAYS CERTAIN THINGS ABOUT IT.

MR. HASLAM: JUST SO THERE IS NO CONFUSION, I'LL TRY TO CLEAR UP IF THERE IS ANY.

Q. IN THE PARAGRAPH WHICH YOU HAVE JUST READ, PROFESSOR KONHEIM, AND JUDGE WILLIAMS HAS JUST READ, THE FIRST SENTENCE THAT SAYS THEY HAVE NOT PROVED IT IS COMPUTATIONALLY DIFFICULT. WHAT KIND OF PROOF IS IT YOU'RE UNDERSTANDING THAT THE AUTHORS ARE TALKING ABOUT THERE?

A. I THINK THEY ARE TALKING ABOUT MATHEMATICALLY PROVING.

THE COURT: WELL, THEY SAY ALONG THAT LINE

SOMEPLACE ELSE THAT I READ -- IT WAS DISCUSSED YESTERDAY.

MR. HASLAM: Q. DOES THE REMAINDER OF THAT PARAGRAPH AT WHICH YOU DIRECTED OUR ATTENTION DESCRIBE, THEREFORE, THE ABSENCE OF MATHEMATICAL PROOF THE METHOD BY WHICH ONE MUST DETERMINE WHETHER A SYSTEM PROVIDES SECURE COMMUNICATION?

A. YES. HIS HONOR READ THE LAST THREE SENTENCES WHICH BEGIN "FAITH IN THE SECURITY OF THESE SYSTEMS MUST THEREFORE REST UPON INTUITION AND THE FAILURE OF CONCERTED ATTEMPTS TO BREAK THEM."

Q. WHAT IS YOUR UNDERSTANDING WHAT IS MEANT BY THE REFERENCE TO "CONCERTED ATTEMPTS TO BREAK THEM"?

A. WELL, I --

THE COURT: DOESN'T IT SPEAK FOR ITSELF?

THE WITNESS: I THINK CONSERTED MEANS MANY PEOPLE.

MR. KENNEDY: OBJECT, MOVE TO STRIKE. BEST EVIDENCE RULE.

THE COURT: I CAN READ AND INTERPRET IT AS I SAID. FAITH IN THE SECURITY SYSTEM MUST THEREFORE REST UPON INTUITION AND THE FAILURE BY PEOPLE TRYING TO -- FAILURE OF A CONCERTED ATTEMPT TO BREAK THEM.

MR. HASLAM: Q. WHO IS IT TO YOUR UNDERSTANDING IN THE ART ARE THE PEOPLE WHO ARE TO

MAKE THESE CONCERTED ATTEMPTS?

THE COURT: PEOPLE THEY'RE TRYING TO KEEP THE SECRETS FROM, AREN'T THEY?

THE WITNESS: THAT'S RIGHT. WELL, ACTUALLY IT DOESN'T REFER, YOUR HONOR, TO EAVESDROPPERS BECAUSE THERE IS NO GROUP -- BUT IN THE SENSE THAT PEOPLE IN THE ACADEMIC COMMUNITY -- INDUSTRY, AM SURE ARE CONCERNED WITH SECURITY.

THE COURT: IT'S A PUBLIC TRANSMISSION, BUT IT'S NOT EAVESDROPPING IN A SENSE. BUT IF SOMEBODY PICKS IT UP AND TRIES TO FIND OUT WHAT IT'S SAYING AND THE SENDER DOESN'T WANT THEM TO KNOW WHAT THEY ARE SAYING.

THE WITNESS: THAT'S RIGHT.

THE COURT: TRYING TO GET THIS INFORMATION THAT THEY DON'T WANT THEM TO HAVE.

MR. HASLAM: IF I COULD JUST GO ON THAT POINT A LITTLE MORE.

Q. THE PURPOSE OF A SECURE CRYPTOGRAPHIC SYSTEM INCLUDING THE ONE THAT WAS PROPOSED IN THE '582 PATENT IS TO PROVIDE PRIVACY OR SECRECY; CORRECT?

A. THAT'S ONE OF THE TASKS OF THE SYSTEM.

Q. IT IS SO THAT, WHEN JUDGE WILLIAMS WANTS TO COMMUNICATE TO SOMEBODY IN A SECURE FASHION, NEITHER YOU OR MR. KENNEDY, NO ONE ELSE CAN LISTENS IN AND

EAVESDROP AND DETERMINE WHAT'S BEING SAID BY JUDGE WILLIAMS AND SOMEBODY ELSE?

A. THAT'S THE INTENDED TASK THAT ENCIPHERMENT IS SUPPOSED TO SOLVE.

Q. AT THE TIME IF I CAME UP WITH A SYSTEM THAT I THOUGHT WOULD BE BETTER THAN ANY PREVIOUSLY PROPOSED TO PROVIDE THAT SECURITY, I COULD WRITE IT UP AND PUBLISH IT; CORRECT?

A. THAT'S RIGHT.

Q. AND I COULD IN MY ARTICLE PROVIDE A MATHEMATICAL PROOF THAT THIS SYSTEM WILL IN FACT GUARANTEE THE PRIVACY OF COMMUNICATION BETWEEN TWO PEOPLE; CORRECT?

A. SUPPOSE YOU COULD.

Q. YOU'VE ALREADY TOLD US THAT THERE IS ONE SYSTEM WHICH DOES THAT.

A. YES.

Q. AS I UNDERSTAND WHAT YOU'RE SAYING IS IS THAT AT THE TIME THAT I PROPOSED MY SYSTEM, IF I CAN'T OR DON'T OFFER MATHEMATICAL PROOF, THAT IN ORDER FOR PEOPLE IN THE FIELD TO GAIN CONFIDENCE THAT WHAT I'VE PROPOSED WILL IN FACT PROVIDE A METHOD OF SECURE COMMUNICATION, IT WOULD BE ONLY AFTER THE SYSTEM I PROPOSED WITHSTOOD CONCERTED ATTEMPTS TO BREAK IT; IS THAT CORRECT?

MR. KENNEDY: OBJECTION, YOUR HONOR. I KNOW

LEADING IS PERMITTED WITH WITNESSES, BUT MR. HASLAM IS TESTIFYING AT THIS POINT. HE'S ALSO ASSUMING FACTS NOT IN EVIDENCE.

THE COURT: IT'S A QUESTION I THINK IT WILL ANSWER ITSELF.

MR. HASLAM: I APOLOGIZE, YOUR HONOR, BUT I WAS CONCERNED THAT -- I'M TRYING TO DRAW THE DIFFERENCE BETWEEN AT THE TIME A SYSTEM IS PROPOSED HOW IT GETS ACCEPTED OR DEMONSTRATED THAT IT IS SECURE.

THE COURT: DIDN'T WE HEAR IN YESTERDAY'S DISCUSSIONS?

MR. HASLAM: THAT'S AFTER IT'S OUT THERE IN USE.

THE COURT: HOW IT WORKS.

MR. HASLAM: Q. IS THIS TALKING ABOUT AT THE TIME IN WHICH IT'S USED, PROFESSOR KONHEIM, OR SOME METHOD WHEREBY PEOPLE IN THE CRYPTOGRAPHIC COMMUNITY ATTEMPT TO ATTACK IT TO DETERMINE WHETHER IT PROVIDES SECURE COMMUNICATIONS OR NOT?

A. SINCE YOU'VE BEEN INTERRUPTED, PERHAPS YOU COULD RESTATE. ARE YOU ASKING ME A QUESTION WHEN THE PAPER IS WRITTEN, WHEN THE PATENT IS SUBMITTED, IF YOU DON'T SUBMIT A PROOF OF -- A MATHEMATICAL PROOF OF SECURITY DO YOU HAVE TO WAIT TO GAIN CONFIDENCE WHEN PEOPLE

ANALYZE THE SYSTEM? IS THAT THE QUESTION?

Q. THAT'S A BETTER QUESTION THAN THE ONE I'VE BEEN TRYING TO FORMULATE.

A. AND NOW YOU HAVE TO ANSWER IT. WELL, THE ANSWER IS YES. THAT IS THE CASE. IF YOU DON'T SUPPLY PROOF, IF THE DRUG MANUFACTURER DOESN'T GIVE AN ABSOLUTE PROOF THAT THIS DRUG IS GOING TO WORK ON THE BASIS OF PHYSICS AND CHEMISTRY, THEN WE'VE GOT TO TEST IT. THE SAME IS TRUE OF A CRYPTOGRAPHIC SYSTEM. JUST SAYING THAT I THINK THE SYSTEM IS VERY HARD IS NOT ENOUGH.

THE COURT: YOU MEAN THE PATENT OFFICE WON'T PATENT IT --

THE WITNESS: THE RULES THAT THE PATENT OFFICE USES MAY BE DIFFERENT. I'M SAYING THAT FOR CRYPTOGRAPHY THAT WHEN YOU WARANTEE THAT A SYSTEM IS GOING TO PROTECT YOUR INFORMATION, THERE'S GOT TO BE SOME EVIDENCE YOU OFFER. ONE OF THE EVIDENCE IS MATHEMATICAL PROOF. THE OTHER EVIDENCE IS THAT PEOPLE IN THE FIELD HAVE EXAMINED THIS AND HAVE FOUND NO METHOD TO BREAK IT.

IF THAT OCCURS AT THE END OF SIX MONTHS, THERE IS SOME CONFIDENCE. IF IT OCCURS AFTER 20 YEARS THAT NO ONE HAS FOUND A METHOD, YOU ARE MUCH MORE CONFIDENT THAT THE INVENTORS OF THE SYSTEM HAVE ACTUALLY FULFILLED THEIR WARANTEE.

THE COURT: FOR A PERIOD OF TIME.

THE WITNESS: FOR A CERTAIN PERIOD OF TIME.

THE COURT: LIKE THE PATENT?

THE WITNESS: PERHAPS FOR THE LENGTH OF THE PATENT, PERHAPS FOR THE INTERVAL OF TIME BETWEEN WHEN IT WAS ISSUED AND WHEN THE PEOPLE BEGAN TO FEEL THAT THERE WAS NO METHOD OF ANALYSIS. BUT THERE'S GOT TO BE SOMETHING IN ABSENCE OF MATHEMATICAL PROOF TO SHOW THAT WHAT YOU ARE OFFERING MEETS THE TEST OF WHAT YOU CLAIM IT TO BE.

SINCE YOU CAN'T PROVE IT MATHEMATICALLY, IT'S GOT TO BE AN EXPERIMENTAL PROCESS. IT'S GOT TO BE AS A RESULT OF PEOPLE STUDYING THE PROBLEM, LOOKING AT IT WITH THEIR EXPERTISE AND DECIDING, YES, THIS SYSTEM I DON'T SEE A WAY OF DOING IT. WELL, IF ONE PERSON DOESN'T SEE IT, THAT'S ONE THING. IF 50 PEOPLE DON'T SEE HOW TO DO IT, IF 50 INDEPENDENT INVESTIGATORS CANNOT FIND OF A WAY OF ANALYZING IT, YOU'RE CERTAINLY MUCH MORE CONFIDENT THAN IF ONE PERSON ANALYZES IT.

MR. HASLAM: Q. ARE THERE ANY OTHER REFERENCES OF WHICH YOU'RE AWARE IN THE ART THAT EITHER AGREE OR DISAGREE OF WHAT YOU'VE JUST TOLD US? AND IN THE INTEREST OF GRAVITY, IF PERHAPS THERE ARE, YOU COULD JUST TELL US THE ARTICLE AND POINT US TO

IT. AND IF THERE ARE ANY QUESTIONS, WE CAN TAKE THEM FROM THERE.

A. I'D BE DELIGHTED TO. EXHIBIT 1000 "NEW DIRECTIONS OF CRYPTOGRAPHY" AGAIN BY WHITFIELD DIFFIE AND PROFESSOR HELLMAN ON PAGE 552 -- EXCUSE ME. I THINK IT'S PAGE 653 NEAR THE TOP OF THE LEFT-MOST COLUMN BEGINNING WITH THE THIRD LINE THE WORDS "AS SYSTEMS."

YOUR HONOR SEES IN THE LEFT-MOST COLUMN THE THIRD LINE. THE SENTENCE THAT BEGINS WITH "AS SYSTEMS"?

THE COURT: "AS SYSTEMS WHOSE STRENGTH HAD BEEN SO ARGUED WERE REPEATEDLY BROKEN, NOTATION OF GIVING MATHEMATICAL PROOFS FOR THESE SECURITY SYSTEMS FELL INTO DISPUTE AND WAS REPLACED BY CERTIFICATION BY WAY OF CRYPTOANALYTIC ASSAULT." THIS IS AN ARTICLE BY WHITFIELD DIFFIE AND MARTY HELLMAN.

MR. HASLAM: Q. CAN YOU JUST TELL US WHAT CRYPTOANALYTIC ASSAULT MEANS?

A. CRYPTOANALYSIS IS THE PROCESS OF TESTING A SYSTEM OF TRYING TO ANALYZE IT.

Q. IS THERE ANYTHING ELSE?

A. OH, YES. THERE ARE OTHER ARTICLES. EXHIBIT 1004, AN ARTICLE ENTITLED "PRIVACY AND AUTHENTICATION" AND "INTRODUCTION TO CRYPTOGRAPHY" BY WHITFIELD DIFFIE AND MARTIN HELLMAN AN INVITED PAPER IN THE PROCEEDINGS

OF THE I TRIPLE E.

DIRECT YOUR HONOR'S ATTENTION TO PAGE 399, THE RIGHT-MOST COLUMN, IT'S THE SECOND PARAGRAPH FROM THE BOTTOM. IT BEGINS WITH THE WORDS "WHILE SOME," PAGE 399, YOUR HONOR.

THE COURT: 399?

THE WITNESS: YOU SEE IN THE RIGHT-HAND COLUMN AT THE VERY BOTTOM, "WHILE SOME."

THE COURT: "THE UNCONDITIONAL COMPUTATIONAL SECURITY"?

THE WITNESS: YES. THAT AGAIN STATES WHAT THE INVENTORS FULLY WELL KNEW.

THE COURT: "TWO FUNDAMENTALLY DIFFERENT WAYS IN WHICH CRYPTOGRAPHIC SYSTEMS MAY BE SECURE"?

THE WITNESS: I'M LOOKING ACTUALLY BELOW THAT, YOUR HONOR.

THE COURT: THAT'S JUST THE FIRST PARAGRAPH?

THE WITNESS: THAT'S IN SECTION D. I WANT THE PARAGRAPH WHICH BEGINS ALMOST AT THE BOTTOM OF THE PAGE, "WHILE SOME UNCONDITIONALLY SECURE."

THE COURT: HOW ABOUT READ THE WHOLE PARAGRAPH INSTEAD OF SOMETHING OUT OF CONTEXT. THIS SAYS "WHILE SOME UNCONDITIONALLY SECURE SYSTEMS CAN BE PROVEN SECURE" -- WE'VE TALKED ABOUT THE DEFINITIONS OF SECURE BEFORE.

THE WITNESS: YES.

THE COURT: "THE THEORY OF COMPUTATIONS COMPLEXITY IS AT PRESENT INADEQUATE DEMONSTRATE THE COMPUTATIONALLY INFEASIBILITY OF ANY CRYPTOANALYTIC PROBLEM. CRYPTOGRAPHY IS THEREFORE FORCED TO RELY ON THE LESS FORMAL CERTIFICATION PROCESS OF SUBJECTING A PERSPECTIVE SYSTEM TO CRYPTOANALYTICAL ASSAULT UNDER THE CIRCUMSTANCES CONSIDERED FAVORABLE TO THE CRYPTOANALYSTS."

THE WITNESS: THAT'S THE PHRASE THAT I WANT TO ADDRESS THE COURT'S ATTENTION.

MR. HASLAM: Q. GOING BACK UP TO THE BEGINNING OF THAT PARAGRAPH, THE SECTION D THAT THE COURT INITIALLY FOCUSED ON, THE SENTENCE SAYS, "THERE ARE TWO FUNDAMENTALLY DIFFERENT WAYS IN WHICH CRYPTOGRAPHIC SYSTEMS MAY BE SECURE." IS THAT BASED ON YOUR REVIEW OF EXHIBIT 1000?

A. REVIEW OF WHAT?

Q. 1004. IS THAT CONSISTENT WITH THE METHOD OF EITHER CERTIFICATION OR MATHEMATICAL PROOF?

A. YES, THAT'S WHAT I THINK THEY REFER, EITHER MATHEMATICAL PROOF OR CERTIFICATION.

THE COURT: THIS ARTICLE IS REFERRED TO AS ONE MARCH 1979. DOES THAT PRECEDE --

THE WITNESS: NO, THAT FOLLOWS THE SUBMISSION

OF THE PATENT.

THE COURT: THE PATENT WAS SUBMITTED BACK WHEN?

MR. HASLAM: OCTOBER 1977.

THE WITNESS: OCTOBER 6, 1977.

MR. HASLAM: EXHIBIT 1004 ON ITS FACE INDICATES THAT THE MANUSCRIPT WAS RECEIVED ON MAY 22, 1978 WHICH IS AGAIN AFTER THE PATENT.

THE COURT: AND THE OTHER ARTICLE WAS 1976.

MR. HASLAM: "NEW DIRECTIONS" WAS -- AT LEAST THIS VERSION WAS NOVEMBER '76. AND EXHIBIT 1000 --

THE WITNESS: 1000, "NEW DIRECTIONS," WAS SUBMITTED JUNE 30, 1976, THAT WAS BEFORE THE FILING DATA.

MR. HASLAM: AND EXHIBIT 1003 WHILE PUBLISHED IN 1978 WAS ON ITS FACE AUGUST 5, 1977, WHICH MEANS THE MANUSCRIPT WAS WRITTEN PRIOR TO THE PATENT BEING FILED.

Q. LET ME ASK YOU JUST TO TAKE A QUICK MOMENT TO TAKE A LOOK AT EXHIBIT 22 TO YOUR DEPOSITION WHICH IS, I BELIEVE, AN EXHIBIT THAT MR. KRAMER SHOWED YOU AT HIS DEPOSITION AND ASKED YOU SOME QUESTIONS ABOUT.

A. EXHIBIT 22. YES, I HAVE THAT IN FRONT OF ME.

Q. AND I BELIEVE IN YOUR DEPOSITION, MR. KRAMER DIRECTED YOUR ATTENTION TO PAGE EIGHT OF THAT EXHIBIT --

AND I APOLOGIZE.

BEFORE WE GET TO PAGE EIGHT, CAN YOU JUST TELL THE COURT BRIEFLY WHAT EXHIBIT 22 IS.

A. EXHIBIT 22 IS A XEROX COPY OF CERTAIN PAGES FROM THE SECOND EDITION OF A BOOK BY BRUCE SNEER. IT'S CALLED "APPLIED CRYPTOGRAPHY," AND IT'S AN OVERVIEW OF CRYPTOGRAPHY WITH EMPHASIS UPON THINGS THAT HAVE TAKEN PLACE IN THE LAST 25 YEARS.

Q. NOW, IF YOU COULD, LOOK AT PAGE EIGHT WHICH IS THE PAGE THAT MR. KRAMER DIRECTED YOUR ATTENTION TO.

A. YES.

Q. THERE'S A HEADING "SECURITY OF ALGORITHMS."

A. YES, I SEE THAT.

Q. AND IS WHAT'S SET FORTH ON THAT PAGE AND IN THAT SECTION CONSISTENT OR INCONSISTENT WITH YOUR TESTIMONY ABOUT HOW ONE GOES ABOUT OR THE METHOD OF DETERMINING WHETHER A CRYPTOGRAPHIC SYSTEM PROVIDES A METHOD OF SECURE COMMUNICATIONS?

A. MAY I JUST TAKE SOME TIME TO LOOK AT THIS?

Q. YES.

A. YES, I THINK THAT THIS IS CONSISTENT WITH WHAT I'VE SAID.

Q. NOW, THERE AT THE BOTTOM OF PAGE EIGHT, THERE'S A REFERENCE TO UNCONDITIONALLY SECURE. VERY BRIEFLY CAN YOU TELL US WHAT THAT IS --

A. UNCONDITIONALLY SECURE -- IT MEANS THAT NO MATTER HOW MUCH CIPHER TEXT THE CRYPTOANALYST HAS, YOU CAN'T EVER RECOVER THE KEY OR THE TEXT OF THE MESSAGE.

Q. BASED ON --

THE COURT: THE NEXT PARAGRAPH "REPORTED FACT ONLY A ONE TIME PASS IS UNBREAKABLE GIVEN INFINITE RESOURCES. ALL OTHER CRYPTOSYSTEMS ARE BREAKABLE IN A CIPHER TEXT ONLY SPECIFIC BY TRYING EVERY POSSIBLE KEY ONE BY ONE AND CHECKING WHETHER RESULTING IN PLAIN TEXT IS MEANINGFUL. THIS IS CALLED A PRUDENT FORCE ATTACK."

MR. HASLAM: Q. DO YOU HAVE AN OPINION AS TO WHETHER THE METHOD OF SECURE COMMUNICATION BEING IN THE '528 PATENT WAS INTENDED BY THE AUTHORS TO BE ONE WHICH WAS UNCONDITIONALLY SECURE?

A. YES, IT WAS NOT INTENDED TO BE UNCONDITIONALLY SECURE.

THE COURT: IT WAS NOT.

THE WITNESS: IT WAS NOT INTENDED NOR IS IT UNCONDITIONAL.

MR. HASLAM: Q. IS THERE ONE, THEN, THAT A METHOD OF SECURE COMMUNICATION PROPOSED IN THE '582 PATENT ONE WHICH YOU BELIEVE WAS INTENDED TO BE COMPUTATIONALLY SECURE?

A. YES. CRUCIAL WORD THE BOOK USES THE

COMPUTATIONALLY SECURE. THAT'S ALSO USED, YOUR HONOR, IN AT LEAST ONE OF THESE ARTICLES THAT WE HAVE LOOKED AT. PROFESSOR HELLMAN AND MR. MERKLE IN THEIR PATENT ALSO USE THE WORD COMPUTATIONALLY INFEASIBLE AS SOMETHING WHICH WOULD PROVE SOMETHING IS COMPUTATIONALLY SECURE. COMPUTATIONALLY SECURE MEANS YOU CAN'T DO ENOUGH COMPUTATION TO BREAK THE SYSTEM.

THE COURT: INFEASIBLE TO --

THE WITNESS: INFEASIBLE TO DO THE COMPUTATION TO BREAK IT.

THE COURT: CONSIDER THE TIME AND COSTS?

THE WITNESS: TIME, COSTS, WHATEVER EQUIVALENT MEASURE THAT YOU WANT TO DO.

THE COURT: WHY DON'T WE TAKE OUR MORNING RECESS AT THIS TIME.

(A 15 MINUTE RECESS WAS TAKEN.)

THE COURT: I DON'T FIND THE LAST EXAMINATION HAS BEEN TOO PRODUCTIVE. YOU'RE NOT FOCUSING ON THE CLAIMS THAT HAVE ANY DIFFERENT MEANING THAN I DO TO IT; SO I'D LIKE AN EXAMINATION OF ANY FURTHER WITNESSES TO POINT TO THE CLAIM. GET RIGHT ON IT BECAUSE WE'VE BEEN TALKING ABOUT SOME THINGS WHICH ARE NOT SERIOUS PROBLEMS.

MR. HASLAM: I APOLOGIZE, YOUR HONOR. I WAS ABOUT TO GO ON. I HAVE THIS BOARD HERE WITH A PORTION

OF CLAIM ONE. PREAMBLE CLAIM ELEMENTS 1,C AND 1,E. THE PREAMBLE STARTS AT "THE METHOD OF COMMUNICATING SECURELY OVER AN INSECURE COMMUNICATION CHANNEL," AND I'VE ELLIPSED THE REST THERE.

THE COURT: THE FACT THAT IT WAS COMMUNICATING A MESSAGE FROM A TRANSMITTER TO A RECEIVER --

MR. HASLAM: Q. PROFESSOR KONHEIM, THERE'S A REFERENCE HERE IN CLAIM ONE TO A METHOD OF COMMUNICATING SECURELY. DO YOU SEE THAT?

A. YES, I DO.

Q. DO YOU HAVE AN OPINION AS TO WHETHER THAT REFERENCE THERE TO A METHOD OF COMMUNICATING SECURELY MEANS A METHOD WHICH IS UNCONDITIONALLY SECURE?

A. AT THIS POINT, IT'S NOT POSSIBLE TO TELL WHETHER THEY ARE REFERRING TO A METHOD OF UNCONDITIONAL SECURITY OR A METHOD OF COMPUTATION INFEASIBILITY.

Q. AND BASED ON YOUR REVIEW OF THE PATENT, THE PROSECUTION HISTORY, DO YOU HAVE AN OPINION AS TO WHETHER THE INVENTORS MEANT TO PROPOSE A METHOD OF COMMUNICATING SECURELY?

THE COURT: THAT DOESN'T HAVE C OR D?

MR. HASLAM: NO, YOUR HONOR. I'VE ADDED THOSE JUST FOR --

THE COURT: IT WOULD BE THE THIRD PARAGRAPH?

MR. HASLAM: THE THIRD PARAGRAPH AND THE FIFTH PARAGRAPH.

THE COURT: PROCESS THE MESSAGE AND THE PUBLIC ENCIPHERING KEY AND THE TRANSMITTER AND GENERATING AN ENCIPHERED MESSAGE.

MR. HASLAM: Q. BASED ON YOUR REVIEW OF THE MATERIALS YOU'VE DESCRIBED FOR US, DO YOU HAVE AN OPINION AS TO WHETHER THE INVENTORS OF THE '582 PATENT WERE PROPOSING A METHOD OF COMMUNICATING SECURELY WHICH WAS UNCONDITIONALLY SECURE AS OPPOSED TO OR COMPUTATIONALLY SECURE?

MR. KENNEDY: OBJECTION, YOUR HONOR. ONE, CALLING FOR SPECULATION. TWO, CALLS FOR A LEGAL CONCLUSION. HE ISN'T BEING ASKED WHAT DO PEOPLE IN THE ART UNDERSTAND. HE'S ASKING THE FACT HOW DOES JUDGE WILLIAMS INTERPRET THIS CLAIM.

THE COURT: WHAT DID YOU HAVE IN MIND? WHAT DOES IT SAY?

MR HASLAM: Q. BASED ON YOUR ANALYSIS, WHAT DO YOU BELIEVE PEOPLE IN THE ART WOULD UNDERSTAND WAS MEANT IN CLAIM ONE BY A METHOD OF COMMUNICATING SECURELY?

A. IN WHAT YOU HAVE LABELED E, IT SAYS "SUCH THAT THE ENCIPHERING TRANSFORMATION IS EASY TO EFFECT BUT COMPUTATIONALLY INFEASABLE TO CONVERT WITHOUT THE SAME

ENCIPHERING KEY." I WOULD READ THAT AS REFERRING TO A SYSTEM WHICH WAS COMPUTATIONALLY SECURE BUT NOT UNCONDITIONALLY.

THE COURT: IT SAYS "COMPUTATIONALLY INFEASIBLE TO CONVERT."

THE WITNESS: THAT MEANS, YOUR HONOR, AT LEAST WHEN I READ IT, IT MEANS IT'S IMPOSSIBLE TO FIND THE SECRET INFORMATION FROM KNOWING JUST THE PUBLIC INFORMATION, AND IT IS INFEASIBLE TO BREAK THE SYSTEM IF I WERE TO PARAPHRASE IT.

THE COURT: OKAY. NEXT QUESTION.

MR. HASLAM: Q. THE METHOD OF COMMUNICATING SECURELY WHICH IS SET FORTH IN CLAIM ONE -- DOES THAT IN YOUR VIEW PROPOSE A METHOD WHICH MEANT -- WOULD THAT BE UNDERSTOOD BY PEOPLE IN THE ART AS PROPOSING A SYSTEM WHICH MEANT THE TWO GOALS THAT YOU SET FORTH AT THE BEGINNING, THAT IT WOULD HIDE INFORMATION AND HIDE IT FOR A PERIOD OF TIME?

A. I THINK AS THEY USE THE WORD "COMMUNICATING SECURELY," THEY MEAN SOMETHING THAT WOULD HIDE THE INFORMATION, OFFER GUARANTEE OF IT FOR SOME PERIOD OF TIME.

THE COURT: NOT INFINITE BUT A CERTAIN PERIOD.

THE WITNESS: NOT INFINITE BUT THE FACT THAT

THE FINITE COMES FROM MEANING -- WHAT MR. HASLAM HAS SECTION E, THE WORDING "COMPUTATIONALLY INFEASIBLE" MEANS THAT THEY HAVE FORMULATED SOMEWHERE THE CONCEPT OF WHAT TIME IS, AND THEY HAVE MADE THE TIME SUCH THAT THIS ALGORITHM WOULD OFFER GUARANTEE OF SECURITY FOR AT LEAST THAT PERIOD OF TIME.

MR. HASLAM: Q. DOES THE PATENT AT ANYWHERE ADDRESS THAT PERIOD OF TIME?

A. YES, THE PATENT DOES.

Q. CAN YOU POINT OUT TO US WHERE IT DOES.

A. LET ME JUST FIND THE REFERENCE. YOUR HONOR, IN COLUMN 5 BEGINNING WITH LINE 10.

Q. THAT'S OF EXHIBIT 13?

A. YES, THE 582 EXHIBIT, COLUMN 5, LINE 10 BEGINNING WITH THE WORDS "A TASK." NOW, I READ THIS AS FOLLOWING --

THE COURT: I HAVE THE PATENT HERE. GO AHEAD.

THE WITNESS: IT READS "A TASK IS CONSIDERED COMPUTATIONALLY INFEASIBLE IF IT'S COST IS MEASURED EITHER BY TIME, THE AMOUNT OF MEMORY USED, OR THE COMPUTING TIME IS FINITE OR IMPOSSIBLY LARGE." THEN THE AUTHOR GOES BY IMPOSSIBLY LARGE THEY SAY, FOR EXAMPLE --

THE COURT: ARE YOU READING FROM THE PATENT

OR THE ARTICLE?

THE WITNESS: I'M READING FROM THE PATENT, BUT I'M SUPPLYING SOME INTERPRETATION AS I GO ALONG.

MR. HASLAM: Q. WHERE ARE YOU AGAIN?

A. I'M ON COLUMN 5.

THE COURT: THERE ARE SOME HOLES IN MY DOCUMENT TO PUT THE THINGS THROUGH, AND 5 HAS GOT A HOLE RIGHT IN THE MIDDLE OF IT. OKAY. I'VE GOT COLUMN 5.

THE WITNESS: I SAID, "A TASK IS CONSIDERED COMPUTATIONALLY INFEASIBLE" --

THE COURT: OKAY. "A TASK IS CONSIDERED COMPUTATIONALLY INFEASIBLE IF IT IS COST" -- WE TALKED ABOUT THAT.

THE WITNESS: RIGHT. AND NOW THEY ARE GOING TO TELL ME WHAT THE COST IS, AND THEY SAY THE COST -- THEY ARE GOING TO TELL ME WHAT IMPOSSIBLY LARGE MEANS. AND THEY SAY 10 TO THE 30TH OPERATIONS, BUT OPERATIONS IS NOT TIME NOR IS IT MEMORY.

SO THEY NOW ARE GOING TO TELL ME HOW DO I TRANSLATE TIME, OPERATIONS AT THE TIME. THEY SAY WELL, LOOK AT THE EXISTING COMPUTATIONAL METHODS AND EQUIPMENT IN 1977. HOW LONG ON THE BEST EQUIPMENT WOULD IT TAKE TO PERFORM 10 TO THE 30TH OPERATIONS, AND I'VE MADE A ROUGH CALCULATION.

I MAY BE OFF BY EVEN A FACTOR OF 100, BUT I SHOW 10 TO THE 16TH YEARS WAS THE TIME NEEDED TO DO 10 TO THE 30TH OPERATIONS. SO EVEN IF WE MAKE A VERY GENEROUS ESTIMATE FOR THE AUTHORS, THEY ARE TALKING IN TERMS OF MANY, MANY LIFE TIMES.

THE COURT: SO ON THE ORDER OF APPROXIMATELY 10 TO THE 30TH OPERATIONS EXISTING COMPUTATIONAL METHODS OF EQUIPMENT?

THE WITNESS: YES.

THE COURT: THAT'S PLAIN LANGUAGE, ISN'T IT?

THE WITNESS: YES.

THE COURT: AND IF YOU'VE GOT THE FORMULA, YOU'LL KNOW HOW LONG THEY ARE TALKING ABOUT.

THE WITNESS: THAT'S RIGHT, AND THAT'S SOMETHING LIKE 10TH TO THE 16TH YEARS.

THE COURT: HOW MANY THOUSAND IS THAT?

THE WITNESS: NEITHER ONE OF US WILL BE AROUND, YOUR HONOR, AT THAT TIME, BUT IT'S A LONG TIME, MANY MORE THAN THOUSANDS OR MILLIONS OF YEARS.

MR. HASLAM: Q. SINCE THE -- I'LL WITHDRAW THAT.

THE COURT: THE SECOND WAS AUTHENTICATING.

MR. HASLAM: Q. IF I COULD, WHILE I'VE GOT THE BOARD UP HERE, CLAIM NUMBER 1,C STATES "GENERATING FROM SAID RANDUM NUMBERS A SECRET DECIPHERING KEY AS

THE RECEIVER SUCH THAT THE SECRET DECIPHERING KEY IS DIRECTLY RELATED TO AND COMPUTATIONALLY INFEASIBLE AS TO GENERATE FROM THE PUBLIC ENCIPHERING KEY."

SEE THE WORD GENERATING, IN THE PHRASE "GENERATING FROM SAID RANDOM NUMBERS A SECRET DECIPHERING KEY"? DOES THE WORD GENERATING HAVE A WELL-UNDERSTOOD MEANING IN THE ART?

A. IN THE CRYPTOGRAPHIC ART, NO IT DOESN'T HAVE ANY WELL-DEFINED MEANING.

Q. AND DOES "GENERATING FROM SAID RANDUM NUMBERS A SECRET DECIPHERING KEY AT THE RECEIVER" HAVE A WELL-UNDERSTOOD MEANING IN THE ART?

A. NO. WHAT IT SPECIFIES IS SOME SORT OF PROCESS, THE RESULT OF SOME SORT OF PROCESS, BUT IT DOESN'T TELL ME HOW TO DO IT.

Q. LIKEWISE, IF I LOOK AT THE CLAIM ELEMENT 1,E WHICH IS GENERALLY SPEAKING, I BELIEVE, RELATES TO THE ENCIPHERING STEP?

A. YES, THAT REFERS TO ENCIPHERING.

Q. IT REFERS TO "PROCESSING THE MESSAGE IN THE PUBLIC ENCIPHERING KEY AT TRANSMITTER AND GENERATING AN ENCIPHERED MESSAGE BY ENCIPHERING TRANSFORMATION SUCH THAT THE ENCIPHERING TRANSFORMATION IS EASY TO EFFECT BUT COMPUTATIONALLY INFEASIBLE TO INVERT WITHOUT THE SECRET DECIPHERING KEY." DO YOU SEE THAT?

A. YES, I DO.
Q. DOES THE WORD PROCESSING HAVE A MEANING IN THE ART?
A. IT DOESN'T HAVE A PRECISE DEFINED OR EVEN SHARPLY DEFINED MEANING IN CRYPTOGRAPHY.
Q. DOES THE WORD "PROCESSING THE MESSAGE IN THE PUBLIC DECIPHERING KEY AT THE TRANSMITTER" HAVE A WELL-UNDERSTOOD MEANING IN THE ART?
A. NO, IT DOES NOT HAVE A WELL-UNDERSTOOD MEANING. IT'S TOO INDEFINITE, TOO VAGUE.
THE COURT: THE CONTEXT OF WHAT THEY ARE TALKING ABOUT ENCIPHERING A TRANSMITTED MESSAGE, RIGHT?
MR. HASLAM: THAT'S WHAT IT'S TALKING ABOUT. THE QUESTION IS WHETHER THOSE TERMS HAVE WELL-DEFINED MEANINGS IN THE ART AS TO WHAT IS TO BE ESTABLISHED.
THE COURT: IN VIEW OF THE CONTEXT IT PUTS IT TO BETTER USE.
MR. HASLAM: Q. WE'VE TALKED ABOUT PROCESSING. DOES THE CLAIM AS A WHOLE HAVE A WELL-UNDERSTOOD PRECISE MEANING IN THE ART?
A. WELL, THE WAY I READ THE ENTIRE CLAIM ONE IN PARTICULARLY THE SECTION OVER HERE, I CAN GLEAN WHAT THE INVENTORS WANTED TO ACHIEVE. THEY WANTED TO DO AN ENCIPHERED ALGORITHM WITH CERTAIN PROPERTIES, AND

THOSE PROPERTIES, THOSE ATTRIBUTES ARE THE WORDS SUCH THAT YOU HI-LIGHTED.

THOSE ATTRIBUTES ARE IT'S EASY TO ENCIPHER, BUT IT'S VERY DIFFICULT TO INVERT THE EFFECT OF ENCIPHERING, THAT IS, TO DECIPHER WITHOUT THE SECRET DECIPHERING KEY. HOW IT'S TO BE DONE. ANYTHING MORE SPECIFIC IS LEFT UP IN THE AIR.

Q. IS THERE, IN YOUR OPINION, A WELL-UNDERSTOOD MEANING IN THE ART AS TO HOW YOU WOULD ACCOMPLISH THE STEPS SET FORTH IN CLAIM ELEMENT 1,E, DECIPHERING STEP?

A. NO. IN MY OPINION, THERE IS NO WELL-DEFINED UNDERSTOOD INTERPRETATION IN CRYPTOGRAPHY OF THAT.

Q. LIKEWISE, WITH CLAIM ELEMENT 1,C WHICH IS THE STEP THAT GENERALLY RELATES TO GENERATING THE SECRET DECIPHERING KEY, IS THERE A WELL-UNDERSTOOD MEANING IN THE ART AS TO HOW ONE WOULD ACCOMPLISH THAT RESULT?

A. NO.

Q. I WANT TO TURN NOW TO THE --

THE COURT: WE KNOW WHAT A SECRET DECIPHERING KEY IS IN THE ART?

THE WITNESS: YES. WE KNOW WHAT A SECRET DECIPHERING KEY IS, BUT HOW THOSE THINGS INTERACT, WE DON'T HAVE ANY IDEA.

THE COURT: GENERATING DOES NOT MEAN

ESTABLISHING, SPECIFYING?

THE WITNESS: YES, IT CERTAINLY MUST MEAN THAT. YOU DO CERTAIN THINGS TO ACHIEVE CERTAIN RESULTS, BUT IT DOESN'T SAY ANYTHING MORE THAN THAT.

THE COURT: DIRECTLY RELATED TO COMPUTATIONALLY INFEASIBLE TO GENERATE A KEY RELATED TO THE DECIPHERING KEY, COMPUTATIONALLY INFEASIBLE GENERATING.

THE WITNESS: IF I MAY ADD, YOUR HONOR, THE WAY I LOOK AND SEE, FOR EXAMPLE --

THE COURT: I'M TALKING ABOUT C.

THE WITNESS: YOU SAID IN ONE HAND I WANT YOU TO TAKE SOME RANDOM NUMBERS. I WANT YOU TO TAKE IN THE OTHER HAND A SECRET DECIPHERING KEY. I WANT YOU TO PUT THEM TOGETHER, MIX THEM UP. AND OUT OF THIS MIXTURE IS TO COME A PUBLIC ENCIPHERING KEY. AND WHATEVER THE MIXING PROCESS GOES ON, THE PUBLIC ENCIPHERING KEY HAS GOT TO BE DIRECTLY RELATED, TOO, THAT IS, IT MUST HAVE--

THE COURT: THE PUBLIC DECIPHERING KEY DESCRIBED ANYPLACE ELSE?

THE WITNESS: IT'S DESCRIBED IN THE SPECIFICATION AND PART OF THE COMMON LANGUAGE OF CRYPTOGRAPHY IN 1977.

MR. HASLAM: THERE IS A PRIOR CLAIM ELEMENT,

YOUR HONOR, THAT TALKS ABOUT THE PUBLIC KEY.

THE COURT: IT'S NOT THE FIRST TIME IT'S USED. YOU KNOW WHAT A PUBLIC DECIPHERING KEY IS?

THE WITNESS: WE KNOW THAT IS AND WHAT A SECRET DECIPHERING KEY IS.

THE COURT: IT DOESN'T MEAN --

THE WITNESS: MIXING THEM TOGETHER IN SOME WAY TO CREATE THEM, AND IT SAYS WHAT THE ATTRIBUTES OF THAT PROCESS MEANS. IT MEANS THAT THE PUBLIC ONE HAS GOT TO DEPEND UPON THE PRIVATE ONE AND THE RANDUM NUMBERS. AND IF YOU LOOK AT WHAT HAS HAPPENED AFTER YOU'VE DONE THIS PROCESS, YOU CAN'T GO BACKWARDS AND SEE WHAT THE PRIVATE KEY WAS.

THE COURT: THAT GOES LATER ON, NOT IN THIS PARTICULAR PARAGRAPH.

THE WITNESS: COMPUTATIONALLY INFEASIBLE IS REFERRED TO IN TWO PLACES. IF YOU LOOK -- GO BACKWARDS, YOU CAN'T SEE WHAT YOU PUT INTO THIS BOX.

THE COURT: GO AHEAD.

MR. HASLAM: Q. THE LANGUAGE AFTER THE "SUCH THAT" IN CLAIM ELEMENT 1,C, I THINK YOU SAID DESCRIBES SOME ATTRIBUTES THAT THE SECRET DECIPHERING KEY SHOULD HAVE?

A. YES.

Q. IS THERE IN YOUR VIEW A WELL-UNDERSTOOD MEANING IN

THE ART AS TO HOW ONE IS TO BRING ABOUT THE RESULT WHICH IS DESCRIBED WHICH IS THAT THE SECRET DECIPHERING KEY IS DIRECTLY RELATED TO AND COMPUTATIONALLY INFEASIBLE TO GENERATE FROM THE PUBLIC ENCIPHERING KEY?

A. NO.

MR. KENNEDY: OBJECT AND MOVE TO STRIKE AS LEGALLY INCOMPETENT. SO FAR THE MAN HAS -- IN FAIRNESS TO THE WITNESS, WHO IS NOT A PATENT LAWYER -- HE'S DESCRIBED A CLAIM FOR WHAT IT IS. IT DESCRIBES THE INVENTION; IT EXPLAINS THE ATTRIBUTES. BUT UNFORTUNATELY YOU HAVE TO GO TO THE SPECIFICATION TO FIND OUT HOW TO PERFORM THE INVENTION.

AND WE CONFESS, THAT'S TRUE IN THIS CASE AS IT'S TRUE OF EVERY PATENT THAT'S EVER BEEN ISSUED IN THE UNITED STATES. HIS CRITICISM IS APPARENTLY THE WAY PATENTS HAVE BEEN WRITTEN. MR. HASLAM KNOWS BETTER THAN THIS.

MR. HASLAM: THEY HAVE CONTENDED, YOUR HONOR, IN THEIR INSTRUCTIONS THERE IS A WELL-UNDERSTOOD MEANING IN THE ART FOR THESE VAGUE INDEFINITE TERMS, GENERATING AND PROCESSING. WHAT I'VE ASKED THE WITNESS IS DO THEY HAVE WELL-UNDERSTOOD MEANINGS IN THE ART?

YOUR HONOR CAN DETERMINE WHETHER THE

WITNESS'S TESTIMONY ON THIS SUBJECT IS OR IS NOT IRRELEVANT, BUT IT GOES DIRECTLY TO A POINT THAT THEY SAY THERE IS A PRECISE, WELL-UNDERSTOOD DEFINITION OF GENERATING AND PROCESSING.

MR. KENNEDY: YOUR HONOR, I DON'T KNOW IF THE FAULT IS WITH THE QUESTIONER OR THE RESPONDENT. WE'RE NOT GETTING ANSWERING ABOUT UNDERSTANDING ABOUT WORDS. THE WITNESS IS TELLING US FROM READING THIS CLAIM, I UNDERSTAND WHAT THE INVENTION SEEKS TO DO, BUT I CAN'T FIGURE OUT HOW TO DO IT, WHICH WE CAN CONCEDE IS ABSOLUTELY TRUE. BUT THAT ISN'T TAKING US ANYPLACE IN TERMS OF A MARKMAN HEARING. THAT'S WHY WE HAVE CLAIMS AND SPECIFICATIONS BOTH IN PATENTS.

I DON'T UNDERSTAND THE RELEVANCE THAT HE'S DESCRIBING OUR PATENT ACCURATELY. IF YOU LOOK AT THE CLAIM, IT WON'T TELL YOU HOW TO DO IT. IF YOU LOOK AT THE SPECIFICATION, IT WON'T TELL YOU WHAT TO CLAIM. WE COULDN'T HAVE GOTTEN A PATENT ISSUED EXCEPT BY PLAYING BY THE RULES IN THAT WAY.

THIS HAD NOTHING TO DO WITH WHETHER WORDS HAVE A MEANING THAT'S UNDERSTOOD. THAT'S A WHOLE LOT DIFFERENT FROM SAYING "CAN YOU BUILD ONE BY LOOKING AT THE CLAIM."

THE COURT: WE ARE SUPPOSED TO FIND THE MEANING, THE LANGUAGE IN THE CLAIMS. AND THE WITNESS

FEELS THAT MEANING OR LACK OF MEANING AND OTHERS MAY BE DIFFERENT. I'LL DECIDE ACTUALLY WHAT THE MEANING SEEMS IN VIEW OF THE WHOLE CONTEXT OF THE PATENT AND THE WHAT WE'RE TRYING TO ACCOMPLISH --

MR. KENNEDY: YES, YOUR HONOR.

THE COURT: -- WHAT WAS SPECIFICALLY SAID.

MR. HASLAM: JUST BRIEFLY TO COMMENT TO THE ARGUMENT THAT WAS MADE. THERE ARE RULES. WE ALL PLAY BY THEM, AND IT SEEMS TO ME THE LAST TIME I LOOKED THE SUPREME COURT WAS THE FINAL ARBITOR OF THE RULES IN THIS AREA. AND IN THE HALBURTON CASE, THE SUPREME COURT INDICATED THAT LANGUAGE WHICH WAS FUNCTIONAL PARTICULARLY AT THE TIME OF NOVALTY WAS EITHER INVALID BECAUSE IT WAS INDEFINITE.

AND THE CONGRESS CHANGED THAT RESULT WHEN IT PASSED SECTION 112 PARAGRAPH THREE NOW PARAGRAPH SIX WHICH SAID YOU CAN SAVE SUCH CLAIMS BUT ONLY YOU CAN SAVE THEM IF YOU SPECIFY ACTS EITHER IN THE CLAIM OR IN THE SPECIFICATION. AND WHAT MR. KENNEDY SAID IS PRECISELY OUR POINT. YOU CAN'T DETERMINE HOW TO ACCOMPLISH THIS RESULT IN THE CLAIMS. HAVING SAID THAT, I'M PREPARED TO MOVE ON.

THE COURT: OKAY.

MR. HASLAM: Q. I'D LIKE TO NOW TURN TO CLAIM TWO, AND IN THERE YOU'LL SEE THE WORD, I

BELIEVE, "AUTHENTICATING" AND THE PHRASE "AUTHENTICATING THE RECEIVER'S IDENTITY TO TRANSMITTER." DO YOU SEE THAT?

A. YES, I DO.

Q. DO YOU HAVE AN UNDERSTANDING FROM READING THE '582 PATENT AND BASED ON YOUR BACKGROUND AS TO HOW ONE OF ORDINARY SKILL IN THE ART WOULD UNDERSTAND CLAIM TWO'S REFERENCE TO AUTHENTICATING A RECEIVER'S IDENTITY?

A. YES. I BELIEVE AUTHENTICATING THE RECEIVER'S IDENTITY IS A WELL-KNOWN TERM USED IN COMPUTER SECURITY.

Q. WHAT DOES IT MEAN?

A. IT MEANS VERIFYING THE IDENTITY OF THE RECEIVER.

Q. WHAT DO YOU MEAN BY "VERIFYING THE IDENTITY"?

A. FINDING SOME METHOD OF PROOF THAT YOU'RE DEALING WITH THE PERSON WHO CLAIMS TO BE THE RECEIVER.

Q. DOES IT MEAN ANYTHING MORE THAN ESTABLISHING THAT THE PERSON WITH WHOM YOU'RE COMMUNICATING HAS THE SECRET DECIPHERING KEY?

A. I'M NOT SURE IF I UNDERSTAND THE QUESTION. I SAID THAT I THINK AUTHENTICATING MEANS VERIFYING THE IDENTITY. IF YOU'RE ASKING ME IF I HAVE THE SECRET DECIPHERING KEY, IS THAT PROOF OF THE IDENTITY? AND THE ANSWER IS NO.

Q. WHY NOT?

A. WELL, ANYONE CAN HAVE A SECRET DECIPHERING KEY. THE WAY IN WHICH THE AUTHENTICATING IS TO BE USED AS DESCRIBED IN THIS CLAIM IS, IF YOU WANT TO SEND ME, YOUR HONOR, A MESSAGE, YOU HAVE RECEIVED FROM MY CLAIM ONE MY PUBLIC ENCIPHERING KEY. YOU'VE RECEIVED THAT IN CLAIM ONE IN PARAGRAPH FOUR, "COMMUNICATING THE PUBLIC ENCIPHERING KEY FROM THE RECEIVER TO THE TRANSMITTER"; SO YOU'VE RECEIVED SOMETHING FROM ME.

I HAVE THAT PRIVATE DECIPHERING KEY, BUT YOU DON'T KNOW THAT YOU'RE TALKING TO ME. YOU KNOW THAT YOU HAVE RECEIVED FROM SOMEONE WHO CALLS HIMSELF ALAN KONHEIM A KEY. YOU'RE GOING TO SEND INFORMATION TO ME ENCIPHERED IN THAT KEY, AND I'M GOING TO OBVIOUSLY BE ABLE TO DECIPHER IT BECAUSE I'VE SENT YOU THE KEY.

BUT YOU DON'T KNOW THAT YOU'RE DEALING WITH ALAN KONHEIM. YOUR CLERK DID NOT ASK ME TO SHOW MY DRIVER'S LICENSE BEFORE I WAS SWORN IN. THIS GENTLEMAN OVER HERE DOESN'T EVEN KNOW IF I'M ALAN KONHEIM. MAYBE I'M MARTIN HELLMAN. SO I MIGHT BE SOMEONE ELSE.

WHAT SHOULD HAVE BEEN DONE IS I SHOULD HAVE OFFERED PROOF THAT I WAS ALAN KONHEIM. AND SO THIS CLAIM OVER HERE DOES NOT AUTHENTICATE THE RECEIVER'S IDENTITY. IT AUTHENTICATES NOTHING. IT JUST USES THE KEY THAT THE RECEIVER HAS DELIVERED TO THE SENDER AND

NOTHING MORE.

Q. IS THERE ANYTHING IN THE SPECIFICATION OF THE '582 PATENT WHICH ADDRESSES THE ISSUE OF VERIFYING THE IDENTITY OF THE PERSON?

A. YES. ON COLUMN 18, BEGINNING IN LINE 46, IT SAYS "VARIATIONS ON THE ABOVE DESCRIBED INVOLVEMENT" -- IT GOES ON TO SAY WHAT WE WOULD DO IS GO TO A PUBLIC CERTIFYING AUTHORITY. WE WOULD IDENTIFY OURSELVES. THAT IS, I WOULD SHOW MY DRIVER'S LICENSE, AND I WOULD DEPOSIT MY KEY AT THAT CERTIFYING OFFICE. THE CERTIFYING OFFICE WOULD SAY YES, I'VE RECEIVED THE KEY FROM ALAN KONHEIM.

THEN WHEN YOU WERE TO AUTHENTICATE MY IDENTITY, YOU WOULD LOOK IN THAT PUBLIC CERTIFYING DIRECTORY AND TO VERIFY THE KEY THAT I GAVE YOU WAS THE KEY WHICH IS ASSOCIATED WITH MY NAME. SO WE PROVE SO IT WOULD PROVIDE THE CHECK THAT SOMEONE ELSE IS NOT TRYING TO IMPERSONATE ME.

Q. IS THERE ANYTHING THAT YOU'VE REVIEWED CONTEMPORANEOUS WITH THE FILING OF THE APPLICATION OF THE '582 PATENT WHICH CONFIRMS OR DOES NOT CONFIRM YOUR VIEW OF THAT'S HOW AN AUTHENTICATION WOULD BE UNDERSTOOD IN THE ART?

A. WELL, I THINK IN SEVERAL OF THE PAPERS, THE AUTHORS REPEAT IN ESSENCE THESE THINGS IN -- LET ME

JUST SEE IF I CAN FIND THE APPROPRIATE CITATION. I'M NOT SURE -- OUTSIDE OF THE PATENT THEY HAVE REPEATED SOME OF THESE IDEAS.

ANYWAY, I THINK THIS IDEA OF HAVING AN OUTSIDE AUTHORITY PROVIDE A CHECK ON THE KEY IS SOMETHING THAT'S VERY WELL UNDERSTOOD IN CRYPTOGRAPHY TODAY. FOR EXAMPLE, IN THE PAPER "HIDING INFORMATION AND SIGNATURES IN TRAPDOOR KNAPSACKS," EXHIBIT 1003, ON PAGE 527, THEY IN ESSENCE -- FIRST OF ALL, THEY --

THE COURT: WHAT EXHIBIT WAS THAT?

THE WITNESS: EXHIBIT 1003 ON PAGE 527, YOUR HONOR, IN PARAGRAPH FIVE, THE BOTTOM OF PAGE 527 IN THE RIGHT-HAND COLUMN. IT FIRST OF ALL --

MR. HASLAM: Q. WAIT A MINUTE.

A. THEY FIRST OF ALL -- FIRST OF ALL SAYING THE LAST LINE, THEY GIVE A SYNONYM FOR AUTHENTICATE. THEY SAY "VERIFY (AUTHENTICATE)," AND THEN THEY DESCRIBE IN SOMEWHAT MORE DETAIL THAT WAS DONE IN COLUMN 18 HOW THEY WOULD HAVE A SYSTEM WHICH WOULD VERIFY (AUTHENTICATE) THE IDENTITY IN AUTHENTICATION.

Q. IS THE METHOD DESCRIBED IN EXHIBIT 1003 SIMILAR TO OR CONSISTENT WITH THAT DESCRIBED IN THE PATENT FOR IDENTIFYING OR AUTHENTICATING A PERSON'S IDENTITY?

A. YES, IT IS. I MIGHT ADD IF I MAY --

THE COURT: IS THERE A QUESTION?

THE WITNESS: THERE IS A PROBLEM WITH CLAIM ONE OVER HERE. YOU OMITTED THE PART B WHICH REFERS TO THE GENERATING USING RANDUM NUMBERS TO GENERATE A PUBLIC ENCIPHERING KEY.

MR. HASLAM: Q. THAT'S THE STEP THAT PRECEDES CLAIM ELEMENT 1,C?

A. YES. I CAN'T SEE HOW IT'S POSSIBLE TO DO B BEFORE C.

Q. BY THAT DO YOU MEAN THAT YOU CANNOT FOLLOW THE STEPS IN THE ORDER LAID OUT IN CLAIM ONE?

A. ABSOLUTELY NOT. YOU CANNOT GET THE PUBLIC KEY FIRST AND THEN THE PRIVATE KEY. IT MUST ALWAYS BE DONE IN THE REVERSE DIRECTION.

Q. IS THERE ANYTHING IN CLAIM ONE WHICH SUGGESTS THAT THERE IS AN ORDER IN WHICH THE STEPS WERE TO BE DONE?

A. WELL, I MEAN IT'S CERTAINLY TRUE THAT YOU'VE FIRST GOT TO ENCIPHER THE MESSAGE BEFORE YOU TRANSMIT IT. SO THERE ARE CERTAIN ACTUAL THINGS THAT COME IN THE ORDER. AND SO THESE STEPS THAT ARE WRITTEN DOWN HERE ARE IN ORDER EXCEPT FOR THE SECOND AND THIRD APPEAR TO BE INVERTED.

FIRST OF ALL, YOU HAVE TO HAVE THE RANDOM NUMBERS BEFORE YOU USE THEM. THEN AFTER YOU HAVE THE RANDUM NUMBERS, IF YOU GET AN ENCIPHERING KEY, YOU HAVE TO HAVE THE KEY BEFORE YOU ENCIPHER. SO THAT

CERTAINLY HAS GOT TO COME BEFORE LATER SECTIONS OF CLAIM ONE. BUT TWO AND THREE APPEAR TO ME TO BE INVERTED.

Q. BY TWO AND THREE YOU MEAN PUBLIC KEY AND PRIVATE KEY?

A. YES. AND WHAT MAKES IT EVEN MORE CURIOUS IS THAT IN CLAIM SEVEN THEY GOT THE ORDER CORRECT.

MR. KENNEDY: YOUR HONOR, OBJECT AND MOVE TO STRIKE. ONE, HE'S WRONG. BUT EVEN IF HE WERE CORRECT, IT HAS NOTHING TO DO WITH MARKMAN.

THE COURT: OVERRULED.

MR. HASLAM: I HAVE NO FURTHER QUESTIONS.

THE COURT: THAT'S ALL? ANY QUESTIONS?

MR. KENNEDY: OH, YES.

THE COURT: HOW LONG DO YOU THINK YOU'D BE?

MR. KENNEDY: MORE THAN SEVEN MINUTES.

THE COURT: MY QUESTION WAS DO YOU WANT TO PROCEED NOW OR WAIT UNTIL AFTER LUNCH? IT'S UP TO YOU.

MR. KENNEDY: IT WOULD BE SIMPLER IF WE RELEASED AND PROBABLY BE MORE EXPEDITIOUS.

THE COURT: LUNCH IN AN HOUR. IS ONE HOUR ENOUGH FOR LUNCH?

(A LUNCH RECESS WAS TAKEN AT 11:55 A.M. TO BE